

# The Complexity of Partition Functions on Hermitian matrices

Marc Thurley\*  
 Computer Science Division  
 University of California  
 Berkeley CA 94720-1776, U.S.A.  
 thurley@eecs.berkeley.edu

April 8, 2010

## Abstract

Partition functions of certain classes of “spin glass” models in statistical physics show strong connections to combinatorial graph invariants. Also known as *homomorphism functions* they allow for the representation of many such invariants, for example, the number of independent sets of a graph or the number nowhere zero  $k$ -flows.

Contributing to recent developments on the complexity of partition functions [GGJT09, CCL09] we study the complexity of partition functions with complex values. These functions are usually determined by a square matrix  $A$  and it was shown in [GGJT09] that for each real-valued symmetric matrix, the corresponding partition function is either polynomial time computable or  $\#P$ -hard.

Extending this result, we give a complete description of the complexity of partition functions definable by Hermitian matrices. These can also be classified into polynomial time computable and  $\#P$ -hard ones. Although the criterion for polynomial time computability is not describable in a single line, we give a clear account of it in terms of structures associated with Abelian groups.

---

\*This work was supported in part by the Deutsche Forschungsgemeinschaft within the research training group Methods for Discrete Structures (GRK 1408) and by a fellowship within the Postdoc-Programme of the German Academic Exchange Service (DAAD).

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Examples. . . . .	3
1.2	Complexity . . . . .	4
<b>2</b>	<b>Preliminaries</b>	<b>6</b>
2.1	Basic Notation . . . . .	6
2.2	Generalized Partition Functions . . . . .	8
<b>3</b>	<b>The Proof of the Main Theorem — An Itinerary</b>	<b>9</b>
3.1	From the General Case to Connected Matrices . . . . .	9
3.2	From Connected Matrices to Hadamard Components . . . . .	10
3.3	Hadamard Components . . . . .	11
3.4	The Polynomial Time Case . . . . .	15
3.5	The Proof of Theorem 1.2 . . . . .	15
<b>4</b>	<b>Basic Technical Results</b>	<b>16</b>
4.1	General Principles . . . . .	16
4.2	Technical Lemmas . . . . .	17
4.2.1	Twin Reduction. . . . .	18
4.2.2	Root Of Unity Transfer . . . . .	19
4.3	The Arithmetical Structure Lemma . . . . .	20
4.3.1	The Proof of Lemma 3.1 . . . . .	21
4.4	Pinning Vertices . . . . .	23
4.4.1	The Reconstruction Lemma . . . . .	23
4.4.2	The Proof of The Pinning Lemma. . . . .	29
4.5	Basic Complexity Results for Congruential Partition Functions . . . . .	31
<b>5</b>	<b>Connected Hermitian Matrices</b>	<b>35</b>
5.1	Satisfying Shape Conditions <b>(C1)</b> and <b>(D1)</b> . . . . .	39
5.2	The Remaining Conditions <b>(C2)</b> , <b>(D2)</b> and <b>(D3)</b> . . . . .	45
5.3	Finishing the Proof of Lemma 5.1 . . . . .	51
<b>6</b>	<b>Hadamard Components</b>	<b>51</b>
6.1	The Group Condition <b>(GC)</b> . . . . .	52
6.2	The Representation Conditions <b>(R1)</b> through <b>(R5)</b> . . . . .	54
6.3	The Affinity Condition <b>(AF)</b> . . . . .	57
6.4	The Proof of the Non-Bipartite Case Lemma 6.1 . . . . .	65
<b>7</b>	<b>Polynomial Time Computable Partition Functions</b>	<b>65</b>
7.1	A Polynomial Time Computable Problem . . . . .	65
7.2	Computing Partition Functions — The Non-Bipartite Case . . . . .	66
7.2.1	The Structure of the Mappings $\rho_c$ . . . . .	66
7.2.2	The Final Reduction . . . . .	69
7.2.3	The proof of Lemma 7.1 . . . . .	70

## 1 Introduction

We study the complexity of *partition functions* (or *homomorphism functions*) on Hermitian<sup>1</sup> matrices — a class of partition functions which has been studied recently in [LS08]. Let  $A \in \mathbb{C}^{m \times m}$  be a Hermitian matrix and  $D \in \mathbb{R}^{m \times m}$  a diagonal matrix with positive diagonal. Let  $G = (V, E)$  be a directed graph with possibly multiple edges. The *partition function*  $Z_{A,D}$  on  $G$  is defined by

$$Z_{A,D}(G) = \sum_{\sigma: V \rightarrow [m]} \prod_{uv \in E} A_{\sigma(u), \sigma(v)} \prod_{v \in V} D_{\sigma(v), \sigma(v)}. \quad (1)$$

It is important to note that the product over edges  $uv \in E$  counts multiplicities as well. If the matrix  $A$  is symmetric, the direction of edges in  $G$  does not affect the value of the partition function. We may then think of  $G$  likewise as an undirected graph. In general, however, the partition function is well-defined only on digraphs. We refer to  $D$  also as a *diagonal matrix of vertex weights* and usually we omit it from the subscript of  $Z_{A,D}$  if it is the identity matrix. Elements of  $[m]$  are called *spins* and mappings  $\sigma : V \rightarrow [m]$  which assign a spin to every vertex of  $G$  are *configurations*. Let  $\mathbb{C}_{\mathbb{A}}$  denote the set of algebraic numbers and let  $\mathbb{R}_{\mathbb{A}}$  be the algebraic reals.

In this paper we study the complexity of partition functions of the form  $Z_{A,D}$  for a Hermitian matrix  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  and a diagonal matrix  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  with positive diagonal. Our main result (cf. Theorem 1.2, below) is a complete complexity classification of these functions.

### 1.1 Examples.

There are several well-known examples of graph-invariants representable by partition functions. Let  $G = (V, E)$  be a digraph. The number of independent sets of  $G$  is given by  $Z_S(G)$  where  $S$  is a  $2 \times 2$  matrix which satisfies  $S_{11} = 0$  and it is one in all other positions. If  $A$  is the adjacency matrix of a  $k$ -clique without self-loops, then  $Z_A(G)$  is the number of  $k$ -colorings of  $G$ .

It will be convenient now and in the following to consider matrices likewise as weighted (directed) graphs such that entry  $A_{ij}$  is the weight of edge  $ij$  and this value being zero denotes absence of an edge. Viewed this way,  $Z_A(G)$  is the number of homomorphisms from  $G$  to (the digraph represented by)  $A$ .

There is an important connection between partition functions and the *Tutte polynomial*. Let  $G = (V, E)$  be a graph. For some subset  $A \subseteq E$  of edges, let  $c(A)$  denote the number of components of the graph  $(V, A)$ , then the *Tutte polynomial* of  $G$ , with parameters  $q, v$  is defined by

$$T(G; q, v) = \sum_{A \subseteq E} q^{c(A)} v^{|A|}.$$

If the value  $q$  is a positive integer then this is also known as the partition function of the  $q$ -state Potts model. By expanding the above sum over components of  $G$ , it can also be shown that, for  $A = J_q + v \cdot I_q$ , we have  $T(G; q, v) = Z_A(G)$ . Here,  $J_q$  denotes the all-ones  $q \times q$  matrix and  $I_q$  the  $q \times q$  identity matrix. In fact this is also an exact correspondence since (see [FLS07])  $q \in \mathbb{N}$  is the only way for which  $T(G; q, v) = Z_A(G)$  for a symmetric real-valued  $A$ .

<sup>1</sup>That is,  $A_{ij} = \overline{A_{ji}}$  for all  $i, j$ , where  $\bar{a}$  denotes complex conjugate.

**Flows and Hermitian Matrices.** Let us turn to an example motivating partition functions on Hermitian matrices. We start with a simple example (which can be found e.g. in [dlHJ93]), given by the matrices

$$U = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \quad D_U = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}. \quad (2)$$

It is not hard to see that, for connected  $G$ , the value  $Z_{U,D_U}(G)$  equals the characteristic function of Eulerian graphs. That is, it is 1 if  $G$  is Eulerian and 0 otherwise. We will see a proof of this in the more general setting of *flows* which we will introduce now.

Usually the representability of *nowhere zero flows* by partition functions is derived via the Tutte polynomial which has strong connections to both. Deviating from this, a direct derivation of this correspondence has been given in [FLS07].

Let  $\mathfrak{G}$  be a finite Abelian group and  $S \subseteq \mathfrak{G}$  any subset. For some oriented graph  $G = (V, E)$  a mapping  $\phi : E \rightarrow S$  and a  $v \in V$  let

$$\partial_\phi(v) = \sum_{uv \in E} \phi(uv) - \sum_{vu \in E} \phi(vu) \quad (3)$$

Such an assignment  $\phi$  is called an  $S$ -*flow*, if  $\partial_\phi(v) = 0$  holds for every vertex  $v \in V$ . For some oriented graph  $G$  let  $f_{S,\mathfrak{G}}(G)$  denote the number of  $S$ -flows (w.r.t.  $\mathfrak{G}$ ) in  $G$ . Let  $\mathfrak{G}^*$  denote the character group of  $\mathfrak{G}$ . The functions  $f_{S,\mathfrak{G}}$  relate to partition functions in the following way. Define two matrices with indices in  $\mathfrak{G}^*$ : a matrix  $A$  and a diagonal matrix  $D$  given by

$$D_{\chi\chi} = |\mathfrak{G}|^{-1} \quad \text{and} \quad A_{\chi,\chi'} = \sum_{g \in S} \overline{\chi(g)} \cdot \chi'(g) \quad (4)$$

It is not too hard to show that (see [FLS07] for details) for every oriented graph  $G$  we have  $Z_{A,D}(G) = f_{S,\mathfrak{G}}(G)$ . If we stipulate that  $S$  be closed under inversion then  $A$  is real-valued and symmetric. The orientation of  $G$  is then inessential. Particularly, if  $S = \mathfrak{G} \setminus \{0\}$  then  $Z_{A,D}(G)$  is the number of *nowhere-zero  $\mathfrak{G}$ -flows* of  $G$ . Since this value depends only on the order  $k = |\mathfrak{G}|$  of  $\mathfrak{G}$ , this counts *nowhere-zero  $k$ -flows* of  $G$ .

If  $S$  is not closed under inversion, then generally  $A$  is not merely a real symmetric matrix: Let, for example  $\mathfrak{G} = \mathbb{Z}_3$  and  $S = \{2\}$ . Define  $\zeta = \exp(2\pi i/3)$ , and consider the character group  $\mathfrak{G}^*$  given by  $\chi_0 = (1, 1, 1)$ ,  $\chi_1 = (1, \zeta, \zeta^2)$  and  $\chi_2 = (1, \zeta^2, \zeta)$ . The definition of  $A$  is given by  $A_{i,j} = \overline{\chi_i(2)} \cdot \chi_j(2)$  which yields

$$A = \begin{pmatrix} 1 & \zeta^2 & \zeta \\ \zeta^{-2} & 1 & \zeta^{-1} \\ \zeta^{-1} & \zeta & 1 \end{pmatrix}.$$

## 1.2 Complexity

A general study of the complexity of partition functions has developed only quite recently, although some instances of these functions can be found among the first problems studied in the context of counting complexity. It follows, for example, from a result of Simon [Sim77] that computing the number of independent sets in a graph is  $\#P$ -hard. This has also been derived independently by Provan and Ball [PB83]. The  $\#P$ -completeness of counting  $k$ -colorings for all  $k \geq 3$  is shown by Linial in [Lin86].

More general complexity results which have a connection to partition functions have been obtained by Jerrum and Sinclair [JS93] who show in particular that the partition function of the 2-state Potts model is  $\#P$ -hard to compute. Related to this, Jaeger, Vertigan and Welsh [JVW90] study the complexity of computing the Tutte polynomial.

Results directly related to our work have strong motivational connections to research in constraint satisfaction problems (CSP) (see e.g. [FV98, Bul06, BK09]). As a matter of fact partition functions and related objects are instances of weighted generalizations of the *counting* constraint satisfaction problem ( $\#CSP$ ).

Of particular interest are *dichotomy results* in the spirit of Schaefer's [Sch78] classical result on Boolean CSP: Depending on the structure of the constraints allowed in a CSP instance, each of these problems is either in  $P$  or  $NP$ -complete. That such results are not self-evident was shown by Ladner [Lad75]: if  $NP$ -hard problems are not polynomial time computable, then there is an infinite hierarchy of problems of increasing difficulty between these extremes. The situation is analogous with counting problems and it is assumed, for example, that counting graph isomorphisms is neither in  $P$  nor  $\#P$ -complete (cf. [Mat79]).

Feder and Vardi [FV98] conjectured that such intermediate complexity is not possible for CSPs. And in fact, the analogous conjecture for the  $\#CSP$  problem has been shown to be true very recently by Bulatov [Bul08] (see also the new proof by Dyer and Richerby [DR10]). Note that the counting analog of Schaefer's result has been obtained much earlier by Creignou and Hermann [CH96] and several weighted extensions of this have been studied recently (see [DGJ09, BDG<sup>+</sup>08, CLX09, DGJR09]).

The line of dichotomy results for partition functions starts with Dyer and Greenhill [DG00] who studied partition functions  $Z_A$  on symmetric  $\{0, 1\}$ -matrices. This is a counting analog of a result by Hell and Nešetřil [HN90]. It turns out that these functions are polynomial time computable only if every component of  $A$  is either a complete bipartite graph, or a complete non-bipartite graph with a loop at every vertex. In all other cases the problem is  $\#P$ -hard.

Bulatov and Grohe [BG05] extended this to a dichotomy for all non-negative symmetric matrices. To state this result, we need to introduce the notion of *blocks* of a matrix  $A$ . Considering  $A$  as a graph, blocks arise naturally as follows: each non-bipartite component corresponds to one block and each bipartite one corresponds to two blocks.

**Theorem 1.1 (Bulatov & Grohe [BG05]).** *Let  $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  be a non-negative symmetric matrix. The following holds.*

- (1) *If every block of  $A$  has rank at most 1 then  $Z_A$  is polynomial time computable.*
- (2) *If  $A$  contains a block of rank at least 2 then  $Z_A$  is  $\#P$ -hard to compute.*

The fact that this result essentially identifies rank 1 matrices as the polynomial time cases renders the result of Bulatov and Grohe widely applicable. Many results on partition functions rely on this theorem, as is the case of Bulatov's result [Bul08]. A further example is the work of Dyer, Goldberg and Jerrum [DGJ08] on *hypergraph partition functions*. Dyer, Goldberg and Paterson [DGP07] give a dichotomy for partition functions  $Z_A$  where  $A$  is an unweighted directed acyclic graph. This has been extended to a dichotomy for all directed  $A$  with non-negative edge-weights by Cai and Chen [CC09].

There are at least two further extensions of the result in [BG05] to be mentioned. Goldberg, Grohe, Jerrum and Thurley [GGJT09] gave a dichotomy theorem for partition functions

$Z_A$  on any symmetric real-valued matrix  $A$ , that is, particularly negative entries in  $A$  are allowed. Furthermore, Cai, Chen and Lu [CCL09] extended this dichotomy yet further to all symmetric complex valued matrices  $A$ .

**The main result of this paper.** Here we will extend the work of [GGJT09] into another natural direction by studying partition functions on Hermitian matrices. Our main result is a dichotomy for these partition functions. As a byproduct, our proof will give a clean account of the algebraic structure underlying the proof of [GGJT09].

**Theorem 1.2.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Then one of the following is true*

- (1) *The function  $Z_{A,D}$  is #P-hard to compute.*
- (2) *The function  $Z_{A,D}$  is polynomial time computable.*

*Furthermore, there is an algorithm which, given  $(A, D)$  decides, whether (1) or (2) occurs.*

Since this work and [CCL09] are both generalizations of the same result [GGJT09] it turns out that the proof structure and the polynomial time cases are rather similar from a high-level point of view. However, the details are quite different in all three proofs.

After some preliminaries presented in the next section, we will give a detailed outline of the proof of this theorem in Section 3. The details of the proofs will then be given in the rest of the paper starting in Section 4.

## 2 Preliminaries

For two counting problems  $A$  and  $B$  we write  $A \leq B$  if there is a polynomial time reduction from  $A$  to  $B$ . If  $A \leq B$  and  $B \leq A$  holds, we write  $A \equiv B$ .

**Computing with Complex Numbers.** Recall that  $\mathbb{C}_{\mathbb{A}}$  denotes the algebraic numbers and  $\mathbb{R}_{\mathbb{A}} = \mathbb{C}_{\mathbb{A}} \cap \mathbb{R}$ . For technical reasons, we will always assume that numbers in  $\mathbb{C}_{\mathbb{A}}$  are given in *standard representation* in some algebraic extension field  $\mathbb{Q}(\theta)$ . That is, we consider numbers in  $\mathbb{Q}(\theta)$  as vectors in a  $d$ -dimensional  $\mathbb{Q}$ -vectorspace, where  $d$  is the degree of  $\mathbb{Q}(\theta)$  over  $\mathbb{Q}$ . It is well-known that for any set of numbers from  $\mathbb{C}_{\mathbb{A}}$  we can compute a  $\theta$  which constitutes the corresponding extension field (cf. [Coh93] p. 181). For further details see also the treatment of this issue in [DGJ08, Thu09].

### 2.1 Basic Notation

For natural numbers  $a \leq b$  we let  $[a, b] := \{a, \dots, b\}$  denote the set of natural numbers from  $a$  to  $b$  and we define  $[b] := [1, b]$ .

**Graphs.** We will be mainly interested in *directed graphs*  $G = (V, E)$  which may have multiple edges. We denote edges by  $uv \in E$ , to explicate that an edge  $e$  has multiplicity  $p$  we sometimes write  $e^p$ . We denote the out-degree (in-degree, resp.) of a vertex  $v$  by  $\deg_G^+(v)$  ( $\deg_G^-(v)$ , resp.). The *degree* of  $v$  is  $d_G(v) = \deg_G^-(v) + \deg_G^+(v)$  in contrast to the *grade*

$\partial_G(v) = \deg_G^+(v) - \deg_G^-(v)$ . A *component* in a digraph  $G = (V, E)$  will be what is usually known as *weakly connected component*.

Let  $G$  be a digraph and  $p \in \mathbb{N}$ . A graph  $G'$  is obtained by *p-thickening*, if each edge  $e \in E$  is replaced by  $p$  many parallel copies of  $e$ . Similarly,  $G'$  is obtained from  $G$  by *p-stretching* if each edge is replaced by a path of length  $p$  — that is, a path on  $p$  edges.

**Matrices and Vectors.** For an  $m \times n$  matrix  $A$  whenever convenient we separate indices by a comma  $A_{i,j}$  to increase readability. Further,  $A_{i,*}$  ( $A_{*,j}$ , resp.) denote the  $i$ th row ( $j$ th column, resp.) of  $A$ . For an  $m \times n$  matrix  $A$  and sets  $I \subseteq [m]$ ,  $J \subseteq [n]$  the matrix  $A_{IJ}$  is obtained from  $A$  by deleting all rows with indices not occurring in  $I$  and all columns not in  $J$ . If  $I = [m]$  ( $J = [n]$ ) we abbreviate this to  $A_{*,J}$  ( $A_{I,*}$ , resp.).

For every  $p \in \mathbb{Q}$  we define the matrix  $A^{(p)}$  by

$$A_{ij}^{(p)} = \begin{cases} (A_{ij})^p & , \text{ if } A_{ij} \neq 0 \\ 0 & , \text{ otherwise.} \end{cases}$$

By  $\text{tr}(A)$  we denote the trace of  $A$  and  $I_m$  is the  $m \times m$  identity matrix. Let  $A$  be an  $m \times n$  matrix and  $A'$  an  $m' \times n'$  matrix. The *tensor product*  $A \otimes A'$  of  $A$  and  $A'$  is the matrix defined as follows. Let the indices be given as pairs  $(i, k) \in [m] \times [m']$  for the row indices and  $(j, l) \in [n] \times [n']$  for the column indices, then

$$(A \otimes A')_{(i,k)(j,l)} = A_{ij} \cdot A_{kl}.$$

With the bijections  $\pi_{\text{row}} : [m] \times [m'] \rightarrow [m \cdot m']$  given by  $\pi_{\text{row}}(i, k) := (i - 1) \cdot m' + k$  and  $\pi_{\text{col}} : [n] \times [n'] \rightarrow [n \cdot n']$  given by  $\pi_{\text{col}}(j, l) := (j - 1) \cdot n' + l$  the pairs translate to ordinary indices. But most often it will be convenient to explicitly refer to the indices as pairs. In this way we will be able to refer to the *tiles* of  $A \otimes A'$  which are the submatrices  $(A \otimes A')_{(i,*)(j,*)} = A_{ij} \cdot A'$ .

The *direct sum* of  $A$  and  $A'$  is the  $(m + m') \times (n + n')$  matrix  $A \oplus A'$  defined by

$$(A \oplus A')_{ij} = \begin{cases} A_{ij} & , \text{ if } i \in [m], j \in [n] \\ A'_{ij} & , \text{ if } i \in [m + 1, m + m'], j \in [n + 1, n + n'] \\ 0 & , \text{ otherwise} \end{cases}$$

Let  $\mathbf{a}, \mathbf{b} \in \mathbb{C}^n$  be vectors. The *scalar product* of  $\mathbf{a}$  and  $\mathbf{b}$  is  $\langle \mathbf{a}, \mathbf{b} \rangle = a_1 \bar{b}_1 + \dots + a_n \bar{b}_n$ . The *Hadamard product* is the vector  $\mathbf{a} \circ \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$ . The *conjugate Hadamard product* is  $\mathbf{a} \bullet \mathbf{b} = \mathbf{a} \circ \bar{\mathbf{b}}$ .

We denote by  $\mathbb{U}$  the set of all complex numbers  $a$  of absolute value 1. The algebraic numbers of absolute values 1 are denoted by  $\mathbb{U}_{\mathbb{A}}$ . Similarly,  $\mathbb{U}_{\omega}$  denotes all  $\omega$ -th roots of unity. A matrix  $A \in \mathbb{U}^{m \times n}$  is called *normalized* if its first row and column are constantly 1. The expression  $\bar{A}$  denotes the *complex conjugate* of  $A$ . A matrix  $A \in \mathbb{U}^{m \times n}$  is called a *complex Hadamard matrix* if  $A \bar{A}^T = n I_n$ , that is all of its rows are pairwise orthogonal. Note that this implies that the columns of  $A$  are pairwise orthogonal as well, which follows from elementary group theory.

**Matrices, blocks and their connection to graphs.** An  $m \times n$  matrix  $A$  is *decomposable*, if there are non-empty index sets  $I \subseteq [m]$ ,  $J \subseteq [n]$  with  $(I, J) \neq [m] \times [n]$  such that  $A_{ij} = 0$  for all  $(i, j) \in \bar{I} \times J$  and all  $(i, j) \in I \times \bar{J}$ . A matrix is *indecomposable* if it is not decomposable and a *block* of  $A$  is a maximal indecomposable submatrix.

Let  $A$  be an  $m \times m$  matrix. The *graph underlying*  $A$  is the digraph defined by  $G_A = ([m], E)$  with  $E := \{ij \mid A_{ij} \neq 0\}$ . For Hermitian matrices the digraph  $G_A$  is symmetric in the sense that  $ij \in E$  iff  $ji \in E$ . For considerations on the connectedness of this graph it is therefore sufficient to consider it as undirected.

We call a matrix  $A$  *connected* if  $G_A$  is connected. We call a submatrix  $A_{II}$  a *component* of  $A$ , if  $G_A[I]$  is a component of  $G_A$ . If  $G_A[I]$  is non-bipartite, then  $A_{II}$  is a block of  $A$ . Note in particular that a connected non-bipartite matrix is a block, and it is thus identical with its *underlying block*. If otherwise  $G_A[I]$  is bipartite then  $A_{II}$  has an *underlying block*  $B$  such that

$$A = \begin{pmatrix} 0 & B \\ \overline{B}^T & 0 \end{pmatrix}.$$

## 2.2 Generalized Partition Functions

Let  $A \in \mathbb{C}^{m \times m}$  be a matrix and  $D \in \mathbb{C}^{m \times m}$  a diagonal matrix. Let  $G = (V, E)$  be some given digraph. A *pinning* of (vertices of)  $G$  with respect to  $A$  is a mapping  $\phi : W \rightarrow [m]$  for some subset  $W \subseteq V$  of vertices of  $G$ . For a given graph  $G = (V, E)$  and a pinning  $\phi$ , we define the *partition function*

$$Z_{A,D}(\phi, G) = \sum_{\phi \subseteq \sigma : V \rightarrow [m]} \prod_{uv \in E} A_{\sigma(u), \sigma(v)} \prod_{v \in V \setminus \text{def}(\phi)} D_{\sigma(v), \sigma(v)}.$$

Note in particular, that the sum is over all configurations  $\sigma : V \rightarrow [m]$  which extend the fixed given pinning  $\phi$  and, for technical reasons, the terms  $D_{\sigma(v), \sigma(v)}$  for  $v \in \text{def}(\phi)$  are excluded from the above expression. The *weight* of the configuration  $\sigma$  is the term  $\prod_{uv \in E} A_{\sigma(u), \sigma(v)} \prod_{v \in V \setminus \text{def}(\phi)} D_{\sigma(v), \sigma(v)}$ . Whenever  $\phi$  is trivial, that is,  $\text{def}(\phi) = \emptyset$  and  $D$  is the identity we omit the terms  $D$  ( $\phi$ , respectively) in the expression. Let  $\text{EVAL}^{\text{pin}}(A, D)$  denote the problem of computing  $Z_{A,D}(\phi, G)$  on input  $G, \phi$ . Analogously,  $\text{EVAL}(A, D)$  denotes the problem restricted to empty input pinnings.

**Congruential Partition Functions.** We say that a matrix  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  is  $\omega$ -*algebraic*, if for every non-zero entry  $A_{ij}$  there is some  $\omega$ -th root of unity  $\zeta$  such that  $A_{ij} = |A_{ij}| \cdot \zeta$ . Working with partition functions on  $\omega$ -algebraic matrices, it will be convenient to transition to a different formulation of such problems.

Let, for a  $d \in \mathbb{Z}$  the expression  $\llbracket d \rrbracket$  denote the modulus of  $d$  after division by  $\omega$ . As  $\omega$  is defined relative to  $A$ , the exact meaning of  $\llbracket d \rrbracket$  will always be clear from context. A family  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_{\omega}}$  of diagonal  $m \times m$  matrices will be called a family of *congruential vertex weights*. The *congruential partition function* on  $A$ , and  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_{\omega}}$ , for a digraph  $G$  and a pinning  $\phi$  is defined by

$$Z_{A, \mathbf{D}}(\phi, G) = \sum_{\phi \subseteq \sigma : V \rightarrow [m]} \prod_{uv \in E} A_{\sigma(u), \sigma(v)} \prod_{v \in V'} D^{\llbracket \partial(v) \rrbracket}_{\sigma(v), \sigma(v)}$$

where  $V' = V \setminus \text{def}(\phi)$ . Recall that  $\partial(v) = \deg^+(v) - \deg^-(v)$  denotes the grade of  $v$  in  $G$ . The connection to ordinary partition functions easily follows from the definitions:



**Lemma 2.1.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian  $\omega$ -algebraic matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Let  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_{\omega}}$  such that  $D^{\llbracket c \rrbracket} = D$  for all  $c \in \mathbb{Z}_{\omega}$ . Then*

$$Z_{A,D}(\phi, G) = Z_{A,\mathbf{D}}(\phi, G) \quad \text{for all digraphs } G \text{ and all pinnings } \phi.$$

Correspondingly,  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  denotes the evaluation problem associated with this partition function on input  $(\phi, G)$ .

### 3 The Proof of the Main Theorem — An Itinerary

We will now give a detailed overview of the most important steps in the proof of Theorem 1.2. Given an arbitrary Hermitian matrix  $A$  and diagonal matrix  $D$  it is rather routine to transition to the case of connected  $A$  and the more general problems  $\text{EVAL}^{\text{pin}}(A, D)$ .

Starting from this point, we will filter the abundance of problems  $\text{EVAL}^{\text{pin}}(A, D)$  until we are left with only the polynomial time computable ones. This process of filtering will be performed by transforming in several steps the problem  $\text{EVAL}^{\text{pin}}(A, D)$  into a problem satisfying certain conditions. In each step more and more such conditions will be accumulated and if any of these conditions fails for a certain problem it will be shown that this is due to the problem being  $\#P$ -hard.

The first step is to gather conditions such that the resulting problem can be transformed into a problem of the form  $\text{EVAL}^{\text{pin}}(A', \mathbf{D})$  where the block underlying the connected matrix  $A'$  is a complex Hadamard matrix (cf. Lemma 3.4) — we call such matrices *Hadamard components*. Once we have achieved this, we will be able to gather more conditions on these problems (cf. Theorem 3.5). And eventually, we will have to solve the non-trivial task of providing a polynomial time algorithm for the remaining problems — Theorem 3.8 yields this.

Some words are in order for the additional statement of Theorem 1.2: It is claimed that there is an algorithm deciding whether given matrices  $A, D$  give rise to polynomial time computable partition functions or  $\#P$ -hard ones. This not very surprising fact will follow straightforwardly from the proof of Theorem 1.2. We give details on the decision algorithm only if they do not follow straightforwardly from the details of the proofs given.

#### 3.1 From the General Case to Connected Matrices

We start by transforming the original problem  $\text{EVAL}(A, D)$  into an equivalent problem  $\text{EVAL}^{\text{pin}}(A', \mathbf{D})$  with  $A'$  an  $\omega$ -algebraic matrix. The transition to  $\omega$ -algebraic matrices is captured by the following lemma. Its proof can be found in Section 4.3.

**Lemma 3.1 (The Arithmetical Structure Lemma).** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. There is an  $\omega \in \mathbb{N}$  and an  $\omega$ -algebraic matrix  $A'$  whose entries satisfy  $|A'_{ij}| \in \mathbb{N}$  and*

$$\text{EVAL}(A', D) \equiv \text{EVAL}(A, D).$$

With the following lemma we then take the step which allows us to pin certain vertices of the input. The proof will be given in Section 4.4.

**Lemma 3.2 (Pinning Lemma).** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Then*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}(A, D).$$

The transition to congruential partition functions is a consequence of Lemma 2.1:

**Corollary 3.3.** *We have  $\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(A, \mathbf{D})$ .*

### 3.2 From Connected Matrices to Hadamard Components

We start under the following preconditions. We are given an  $\omega$ -algebraic Hermitian matrix  $A \in \mathbb{C}^{m \times m}$  which satisfies that  $|A_{ij}| \in \mathbb{N}$  for all  $i, j \in [m]$  however this being in  $\mathbb{N}$  is not essential. We say that a matrix  $H$  and a family of diagonal matrices  $\mathbf{D}$  define an **(H-STD)** problem, if the following holds

**(H-STD)** There are  $n, \omega \in \mathbb{N}$  and  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  is a family of diagonal matrices such that

- $H \in \mathbb{U}_\omega^{n \times n}$  is a normalized Hermitian Hadamard matrix..
- We have  $D^{\llbracket 0 \rrbracket} = I_n$ ,  $D^{\llbracket c \rrbracket} \in (\{0\} \cup \mathbb{U}_{\mathbb{A}})^{n \times n}$  and  $D^{\llbracket -c \rrbracket} = \overline{D^{\llbracket c \rrbracket}}$  for all  $c \in \mathbb{Z}_\omega$ .

Further, an evaluation problem  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is called a **(B-H-STD)**-problem if it satisfies the following conditions.

**(B-H-STD)** There are  $n, \omega \in \mathbb{N}$  such that  $A$  is a connected Hermitian matrix with underlying block  $H$  and  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  is a family of diagonal matrices. Further,

- $H \in \mathbb{U}_\omega^{n \times n}$  is a normalized complex Hadamard matrix.
- For all  $c \in \mathbb{Z}_\omega$  there are diagonal matrices  $D^{\llbracket c \rrbracket, \text{row}}, D^{\llbracket c \rrbracket, \text{col}} \in (\{0\} \cup \mathbb{U}_{\mathbb{A}})^{n \times n}$  such that

$$D^{\llbracket c \rrbracket} = D^{\llbracket c \rrbracket, \text{row}} \oplus D^{\llbracket c \rrbracket, \text{col}}.$$

- $D^{\llbracket 0 \rrbracket} = I_{2n}$ , and  $D^{\llbracket -c \rrbracket} = \overline{D^{\llbracket c \rrbracket}}$  for all  $c \in \mathbb{Z}_\omega$ .

The following lemma shows how we can reduce the complexity classification of evaluation problems on arbitrary connected Hermitian matrices to those on Hadamard components. Its proof will be given in Section 5.

**Lemma 3.4.** *Let  $A$  be a connected  $\omega$ -algebraic Hermitian matrix and  $D$  a diagonal matrix of positive vertex weights. Then either  $\text{EVAL}^{\text{pin}}(A, D)$  is #P-hard or the following holds.*

- (1) *If  $A$  is not bipartite then there is an  $\omega$ -algebraic Hermitian matrix  $H$  and a family of diagonal matrices  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  which define an **(H-STD)** problem such that*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(H, \mathbf{D}).$$

- (2) *If  $A$  is bipartite then there is an  $\omega$ -algebraic Hermitian matrix  $A'$  and a family of diagonal matrices  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  which define a **(B-H-STD)** problem such that*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(A', \mathbf{D}).$$

### 3.3 Hadamard Components

After applying Lemma 3.4 we are left with the task of classifying the complexity of **(H-STD)** and **(B-H-STD)** problems. We will now develop further conditions on these problems which will eventually lead us to polynomial time computable problems. The definition of these conditions will be given in the following. We start with the statement of the theorem whose proof can be found in Section 6.

**Theorem 3.5.** *Let  $A$  be an  $\omega$ -algebraic matrix and  $\mathbf{D}$  a family of diagonal matrices defining either an **(H-STD)** problem or a **(B-H-STD)** problem. Then either  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is  $\#P$ -hard or the following holds.*

- (1) *If  $A, \mathbf{D}$  define an **(H-STD)** problem then they satisfy conditions **(GC)**, **(R1)** through **(R5)** and the Affinity Condition **(AF)**.*
- (2) *If  $A, \mathbf{D}$  define a **(B-H-STD)** problem then they satisfy conditions **(GC)**, **(B-R1)** through **(B-R5)** and the Affinity Condition **(B-AF)**.*

The first condition **(GC)** stipulates that the Hadamard matrix  $H$  underlying every **(H-STD)** and **(B-H-STD)** problem has a certain group structure.

**The Group Structure of  $H$ .** Let  $R(H) := \{H_{i,*} \mid i \in [n]\}$  denote the set of rows of  $H$ . The *Group Condition* is defined as follows.

**(GC)**  $H_{i,*} \circ H_{j,*} \in R(H)$  and  $H_{i,*}^T \circ H_{j,*}^T \in R(H^T)$  for all  $i, j \in [n]$ .

The name “Group Condition” is justified as it guarantees that  $R(H)$  and  $R(H^T)$  are Abelian groups under the Hadamard product  $\circ$ . To see this, note that the definition of **(GC)** is known as the *subgroup criterion for finite groups*.

To introduce all further conditions, we will consider the non-bipartite case of **(H-STD)** problems and the bipartite **(B-H-STD)** problems separately. Let us begin with the non-bipartite case.

**A Group Theoretic Account of (H-STD)-problems.** When we are working with Abelian groups  $\mathfrak{G}$ , unless defined otherwise, the group operation will be denoted by  $+$  and the neutral element will be  $0$ . Let an  $\omega$ -algebraic matrix  $H$  and a family  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{\mathbb{Z}_\omega}$  define an **(H-STD)** problem. Further, assume that  $H$  satisfies the group condition **(GC)**.

Fix the canonical isomorphism  $\mathcal{X}_\omega : \mathbb{Z}_\omega \rightarrow \mathbb{U}_\omega$  where  $\mathbb{U}_\omega$  denotes the set of  $\omega$ -th roots of unity. That is, we have  $\mathcal{X}_\omega(a) = \exp(\frac{2\pi i a}{\omega})$ . By the group condition **(GC)** the set  $R(H)$  of rows of  $H$  is an Abelian group under the Hadamard product. Further by the Fundamental Theorem of Finitely Generated Abelian Groups  $R(H)$  is isomorphic to some Abelian group  $\mathfrak{G} = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_z}$  with  $q_i$  some prime powers.

Note first that the order of each element  $g \in \mathfrak{G}$  divides  $\omega$ . To see this, recall that  $g \in \mathfrak{G}$  corresponds to a row  $H_{i,*}$  by the above mentioned isomorphism. The order of  $H_{i,*}$  is the least common multiple of the orders of its entries  $H_{ij}$ . However, each of these entries is an  $\omega$ -th root of unity.

Let  $f : R(H) \rightarrow \mathfrak{G}$  be an isomorphism. We see particularly that for all  $i \in [n]$  there is a unique  $a \in \mathfrak{G}$  such that  $f(H_{i,*}) = a$  and — as  $H$  is Hermitian —  $f(H_{*,i}) = f(\overline{H_{i,*}}) = -a$ . We

may therefore relabel the entries of  $H$  by elements of  $\mathfrak{G}$  such that  $H_{a,*} \circ H_{b,*} = H_{a+b,*}$  for all  $a, b \in \mathfrak{G}$ . In this way, if for  $i, j \in [n]$  we let  $a, b \in \mathfrak{G}$  be their corresponding group elements, then we have  $H_{ij} = H_{a,-b}$ . We thus obtain  $H_{a,-b} = H_{ij} = \overline{H}_{ji} = \overline{H}_{b,-a}$ .

We further define an operator  $\langle *, * \rangle_\omega : \mathfrak{G} \times \mathfrak{G} \rightarrow \mathbb{Z}_\omega$  such that

$$H_{a,-b} = \mathcal{X}_\omega [\langle a, b \rangle_\omega] \text{ for all } a, b \in \mathfrak{G}.$$

It thus follows directly from our considerations that

**Lemma 3.6.** *The operator  $\langle *, * \rangle_\omega$  has the following properties.*

- For all  $g \in \mathfrak{G}$  the mappings  $\langle g, * \rangle_\omega$  and  $\langle *, g \rangle_\omega$  are group homomorphisms.
- For all  $g, h \in \mathfrak{G}$  we have  $\langle g, h \rangle_\omega = -\langle h, g \rangle_\omega$ .

We summarize these properties by saying that the operator  $\langle *, * \rangle_\omega$  is *skew-bilinear*. Extending this description, we would like to describe the non-zero entries of the diagonal matrices  $D^{\llbracket c \rrbracket}$  in a similar way, although our reasoning so far does *not* allow us to stipulate that  $D_{a,a}^{\llbracket c \rrbracket} \neq 0$  implies  $D_{a,a}^{\llbracket c \rrbracket} \in \mathbb{U}_\omega$ .

Therefore we extend  $\mathbb{Z}_\omega$  to some set  $\Omega$  and  $\mathcal{X}_\omega$  to some mapping  $\mathcal{X} : \Omega \rightarrow \mathbb{U}$  such that for all  $c \in \mathbb{Z}_\omega$  and all  $a \in \mathfrak{G}$ , if  $D_{a,a}^{\llbracket c \rrbracket} \neq 0$  then there is some  $\alpha \in \Omega$  such that  $\mathcal{X}[\alpha] = D_{a,a}^{\llbracket c \rrbracket}$ . We may further assume that  $\Omega$  is itself an Abelian group and  $\mathcal{X}$  is a homomorphism. (Note that this is possible if we just define  $\Omega$  as the real interval  $[0, \omega)$  and  $\mathcal{X}(a) = \exp(\frac{2\pi i}{\omega} \cdot a)$ ). Altogether, from conditions **(H-STD)** and **(GC)** we have derived the following.

- (R1)** There is an Abelian group  $\Omega \supseteq \mathbb{Z}_\omega$  and a homomorphism  $\mathcal{X} : \Omega \rightarrow \mathbb{U}$  such that  $\mathcal{X} \upharpoonright_{\mathbb{Z}_\omega}$  is the canonical isomorphism between the additive group  $\mathbb{Z}_\omega$  and the multiplicative group  $\mathbb{U}_\omega$ .
- (R2)**  $R(H)$  is isomorphic to some Abelian group  $\mathfrak{G} = \mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_z}$  for  $q_1, \dots, q_z$  some prime powers. There is a skew-bilinear operator  $\langle *, * \rangle_\omega : \mathfrak{G} \times \mathfrak{G} \rightarrow \mathbb{Z}_\omega$  such that

$$H_{a,-b} = \mathcal{X} [\langle a, b \rangle_\omega] \text{ for all } a, b \in \mathfrak{G}.$$

Furthermore, the order of each  $g \in \mathfrak{G}$  divides  $\omega$ .

We shall define three further conditions. The first of which will be shown to hold in the following.

- (R3)** For every  $c \in \mathbb{Z}_\omega$  let  $\Lambda_c = \{a \in \mathfrak{G} \mid D_{a,a}^{\llbracket c \rrbracket} \neq 0\}$  be the *support* of  $D^{\llbracket c \rrbracket}$ . Then there is some  $\beta_c \in \mathfrak{G}$  and a subgroup  $\mathfrak{G}_c$  of  $\mathfrak{G}$  such that

$$\Lambda_c = \beta_c + \mathfrak{G}_c.$$

- (R4)** For every  $c \in \mathbb{Z}_\omega$  with  $D^{\llbracket c \rrbracket} \neq 0$  there is a mapping  $\rho_c : \mathfrak{G}_c \rightarrow \Omega$  such that

$$D_{a,a}^{\llbracket c \rrbracket} = \mathcal{X} [\rho_c(a - \beta_c)] \text{ for all } a \in \Lambda_c.$$

- (R5)** For every  $c \in \mathbb{Z}_\omega$  with  $D^{\llbracket c \rrbracket} \neq 0$  we have  $\rho_c(0) = 0$ .

Note that, by the above, condition **(R4)** holds once we made sure that **(R3)** is satisfied. We will define a further criterion on the functions  $\rho_c$  describing the non-zero vertex weights. We call this criterion the *Affinity Condition* for  $D^{\llbracket c \rrbracket}$ :

**(AF)** For all  $c \in \mathbb{Z}_\omega$  there is a mapping  $\gamma_c : \mathfrak{G}_c \rightarrow \mathfrak{G}$  such that following is true. We have

$$\rho_c(y + x) - \rho_c(x) - \rho_c(y) = \langle \gamma_c(y), x \rangle_\omega \text{ for all } x, y \in \mathfrak{G}_c. \quad (5)$$

**A NOTE ON DECIDABILITY.** Apart from the conditions presented in other sections, the decidability of the conditions given here may, at this point, be a bit obscure to the reader. We shall give a bit of insight into this, now. Assume, we are given a matrix  $H$  and a family  $\mathbf{D}$  of diagonal matrices defining an **(H-STD)** problem and we want to decide whether this problem is polynomial time computable. By Theorem 3.5 it turns out that  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is  $\#P$ -hard unless all of the conditions just described are satisfied. To be precise, as we have not given an algorithm which can compute the representation as given in **(R1)** to **(R5)**, for the cases of  $\#P$ -hardness Theorem 3.5 does only prove the existence of such a reduction.

Eventually however, if the evaluation problem is polynomial time computable, it will turn out that each of the matrices  $D^{\llbracket c \rrbracket}$  satisfies the following<sup>2</sup>

$$\text{For all } c \in \mathbb{Z}_\omega \text{ all non-zero entries of } D^{\llbracket c \rrbracket} \text{ are in } \mathbb{U}_{2\omega}. \quad (6)$$

In a first step we may thus check whether this is the case. If so it follows straightforwardly that the Abelian group  $\Omega$  defined in condition **(R1)** is finite and all of the conditions defined can be computed straightforwardly.

**A Group Theoretic Account of (B-H-STD)-problems.** Let  $A$  be an  $\omega$ -algebraic matrix and  $\mathbf{D}$  a family of diagonal matrices define a **(B-H-STD)**-problem. Assume further that the block  $H$  underlying  $A$  satisfies the group condition **(GC)**.

Fix the isomorphism  $\mathcal{X}_\omega : \mathbb{Z}_\omega \rightarrow \mathbb{U}_\omega$  as before. By the group condition **(GC)**, the set  $R(H)$  of rows of  $H$  and the set  $R(H^T)$  of its columns are Abelian groups under the Hadamard product. Hence, by the Fundamental Theorem of Finitely Generated Abelian Groups  $R(H)$  is isomorphic to some Abelian group  $\mathfrak{G}_{\text{row}} = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_z}$  with  $q_i$  some prime powers. Further,  $R(H^T)$  is isomorphic to some Abelian group  $\mathfrak{G}_{\text{col}} = \mathbb{Z}_{q'_1} \oplus \cdots \oplus \mathbb{Z}_{q'_z}$ , with  $q'_i$  some prime powers.

Note first that the order of each element  $g \in \mathfrak{G}_{\text{row}}$  ( $g' \in \mathfrak{G}_{\text{col}}$  resp.) divides  $\omega$ . To see this recall that  $g \in \mathfrak{G}_{\text{row}}$  corresponds to a row  $H_{i,*}$  by the above mentioned isomorphism. The order of  $H_{i,*}$  is the least common multiple of the orders of its entries  $H_{ij}$  and each of these entries is a  $\omega$ -th root of unity.

Let  $f_{\text{row}} : R(H) \rightarrow \mathfrak{G}_{\text{row}}$  and  $f_{\text{col}} : R(H^T) \rightarrow \mathfrak{G}_{\text{col}}$  be group isomorphisms. We see particularly that for all  $i \in [n]$  there is a unique  $a \in \mathfrak{G}_{\text{row}}$  such that  $f_{\text{row}}(H_{i,*}) = a$  and the analogue of this holds for the columns. We may therefore relabel the entries of  $H$  by elements of  $\mathfrak{G}_{\text{row}}$  and  $\mathfrak{G}_{\text{col}}$  such that  $H_{a,*} \circ H_{b,*} = H_{a+b,*}$  for all  $a, b \in \mathfrak{G}_{\text{row}}$  and  $H_{*,c} \circ H_{*,d} = H_{*,c+d}$  for all  $c, d \in \mathfrak{G}_{\text{col}}$ . We further define an operator  $\langle *, * \rangle_\omega : \mathfrak{G}_{\text{row}} \times \mathfrak{G}_{\text{col}} \rightarrow \mathbb{Z}_\omega$  such that

$$H_{a,b} = \mathcal{X}_\omega[\langle a, b \rangle_\omega] \text{ for all } a \in \mathfrak{G}_{\text{row}}, b \in \mathfrak{G}_{\text{col}}.$$

<sup>2</sup>The interested reader may find the proof of this in Lemma 7.4.

Be aware that, although we denote this operator in the same way as the corresponding one in the non-bipartite case, the two operators are different. However, it will always be unambiguously clear from the context, which of the two operators we are referring to.

We say that the operator  $\langle *, * \rangle_\omega$  is *bilinear* if the following holds: For all  $g \in \mathfrak{G}_{\text{row}}$  and all  $g' \in \mathfrak{G}_{\text{col}}$  the mappings  $\langle g, * \rangle_\omega$  and  $\langle *, g' \rangle_\omega$  are group homomorphisms. It follows directly from the above considerations that

**Lemma 3.7.** *The operator  $\langle *, * \rangle_\omega$  is bilinear.*

We would like to describe the non-zero entries of the diagonal matrices  $D^{[\mathbb{C}]}$  in a similar way, although our reasoning so far does *not* allow us to stipulate that  $D_{a,a}^{[\mathbb{C}]} \neq 0$  implies  $D_{a,a}^{[\mathbb{C}]} \in \mathbb{U}_\omega$ . Therefore we extend  $\mathbb{Z}_\omega$  to some set  $\Omega$  and  $\mathcal{X}_\omega$  to some mapping  $\mathcal{X} : \Omega \rightarrow \mathbb{U}$  such that for all  $c \in \mathbb{Z}_\omega$  and all  $a \in [2n]$ , if  $D_{a,a}^{[\mathbb{C}]} \neq 0$  then there is some  $\alpha \in \Omega$  such that  $\mathcal{X}[\alpha] = D_{a,a}^{[\mathbb{C}]}$ . We further assume that  $\Omega$  is itself an Abelian group and  $\mathcal{X}$  is a homomorphism.

Altogether, from conditions **(B–H–STD)** and **(GC)** we have derived the following.

**(B–R1)** There is an Abelian group  $\Omega$  and a homomorphism  $\mathcal{X} : \Omega \rightarrow \mathbb{U}$  such that  $\mathcal{X} \upharpoonright_{\mathbb{Z}_\omega}$  is the canonical isomorphism between the additive group  $\mathbb{Z}_\omega$  and the multiplicative group  $\mathbb{U}_\omega$ .

**(B–R2)**  $R(H)$  is isomorphic to some Abelian group  $\mathfrak{G}_{\text{row}} = \mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_z}$  for  $q_1, \dots, q_z$  some prime powers.  $R(H^T)$  is isomorphic to some Abelian group  $\mathfrak{G}_{\text{col}} = \mathbb{Z}_{q'_1} \oplus \dots \oplus \mathbb{Z}_{q'_z}$  for  $q'_1, \dots, q'_z$  some prime powers. There is a bilinear operator  $\langle *, * \rangle_\omega : \mathfrak{G}_{\text{row}} \times \mathfrak{G}_{\text{col}} \rightarrow \mathbb{Z}_\omega$  such that

$$H_{a,b} = \mathcal{X}[\langle a, b \rangle_\omega] \text{ for all } a \in \mathfrak{G}_{\text{row}}, b \in \mathfrak{G}_{\text{col}}.$$

Furthermore, the order of each  $g \in \mathfrak{G}_{\text{row}}$  and each  $g' \in \mathfrak{G}_{\text{col}}$  divides  $\omega$ .

We shall define three further conditions. The first of which will be shown to hold in the following.

**(B–R3)** For every  $c \in \mathbb{Z}_\omega$  let  $\Lambda_{c,\text{row}} = \{a \in \mathfrak{G}_{\text{row}} \mid D_{a,a}^{[\mathbb{C}],\text{row}} \neq 0\}$  be the *support* of  $D^{[\mathbb{C}],\text{row}}$  and let  $\Lambda_{c,\text{col}} = \{a \in \mathfrak{G}_{\text{col}} \mid D_{a,a}^{[\mathbb{C}],\text{col}} \neq 0\}$  be the *support* of  $D^{[\mathbb{C}],\text{col}}$ . There are  $\beta_{c,\text{row}} \in \mathfrak{G}_{\text{row}}$ ,  $\beta_{c,\text{col}} \in \mathfrak{G}_{\text{col}}$  and subgroups  $\mathfrak{G}_{c,\text{row}}$  of  $\mathfrak{G}_{\text{row}}$  and  $\mathfrak{G}_{c,\text{col}}$  of  $\mathfrak{G}_{\text{col}}$  such that

$$\Lambda_{c,\text{row}} = \beta_{c,\text{row}} + \mathfrak{G}_{c,\text{row}} \quad \text{and} \quad \Lambda_{c,\text{col}} = \beta_{c,\text{col}} + \mathfrak{G}_{c,\text{col}}.$$

**(B–R4)** For every  $c \in \mathbb{Z}_\omega$  there are mappings  $\rho_{c,\text{row}} : \mathfrak{G}_{c,\text{row}} \rightarrow \Omega$  and  $\rho_{c,\text{col}} : \mathfrak{G}_{c,\text{col}} \rightarrow \Omega$  such that

$$D_{a,a}^{[\mathbb{C}],\text{row}} = \mathcal{X}[\rho_{c,\text{row}}(a - \beta_{c,\text{row}})] \text{ for all } a \in \Lambda_{c,\text{row}}.$$

$$D_{a,a}^{[\mathbb{C}],\text{col}} = \mathcal{X}[\rho_{c,\text{col}}(a - \beta_{c,\text{col}})] \text{ for all } a \in \Lambda_{c,\text{col}}.$$

**(B–R5)** For every  $c \in \mathbb{Z}_\omega$  the following holds. If  $D^{[\mathbb{C}],\text{row}} \neq 0$  then  $\rho_{c,\text{row}}(0) = 0$  and if  $D^{[\mathbb{C}],\text{col}} \neq 0$  then  $\rho_{c,\text{col}}(0) = 0$ .

Note that, by the above, condition **(B–R4)** holds once we made sure that **(B–R3)** is satisfied. As in the description of the **(H–STD)** problems we will give a further condition on the mappings  $\rho_{c,\text{row}}, \rho_{c,\text{col}}$  describing the non-zero vertex weights. Again, we call this the *Affinity Condition* for  $D^{[\mathbb{C}]}$ , which reads

**(B–AF)** For all  $c \in \mathbb{Z}_\omega$  there are mappings  $\gamma_{c,\text{row}} : \mathfrak{G}_{c,\text{row}} \rightarrow \mathfrak{G}_{c,\text{col}}$  and  $\gamma_{c,\text{col}} : \mathfrak{G}_{c,\text{col}} \rightarrow \mathfrak{G}_{c,\text{row}}$  such that the following is true.

$$\rho_{c,\text{row}}(y + x) - \rho_{c,\text{row}}(x) - \rho_{c,\text{row}}(y) = \langle x, \gamma_{c,\text{row}}(y) \rangle_\omega \text{ for all } x, y \in \mathfrak{G}_{c,\text{row}} \quad (7)$$

$$\rho_{c,\text{col}}(y + x) - \rho_{c,\text{col}}(x) - \rho_{c,\text{col}}(y) = \langle \gamma_{c,\text{col}}(y), x \rangle_\omega \text{ for all } x, y \in \mathfrak{G}_{c,\text{col}}. \quad (8)$$

DECIDABILITY. Note that the question whether a given **(B–H–STD)** problem is polynomial time computable or  $\#P$ -hard can be solved analogously to the non-bipartite case. Recall the discussion given there.

### 3.4 The Polynomial Time Case

By now we have arrived at **(H–STD)** problems and **(B–H–STD)** problems satisfying all conditions we have defined so far. It remains to show that this implies polynomial time computability of the corresponding problems.

**Theorem 3.8.** *Let  $A$  be an  $\omega$ -algebraic matrix and  $\mathbf{D}$  a family of diagonal matrices. The problem  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is polynomial time computable if the following holds.*

- (1) *If  $A, \mathbf{D}$  define an **(H–STD)** problem then they satisfy conditions **(GC)**, **(R1)** through **(R5)** and the Affinity Condition **(AF)**.*
- (2) *If  $A, \mathbf{D}$  define a **(B–H–STD)** problem then they satisfy conditions **(GC)**, **(B–R1)** through **(B–R5)** and the Affinity Condition **(B–AF)**.*

This theorem will follow by reducing the partition functions satisfying the above conditions to a problem which has been shown to be polynomial time computable in [CCL09]. The proof details will be given in Section 7.

### 3.5 The Proof of Theorem 1.2

With the high-level results we have derived in the previous sections we are now able to prove the Main Theorem 1.2. In a first step, let us show how we can easily derive the result for problems  $\text{EVAL}^{\text{pin}}(A, D)$  on connected matrices  $A$ .

**Lemma 3.9.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a connected  $\omega$ -algebraic Hermitian matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Then either  $\text{EVAL}^{\text{pin}}(A, D)$  is  $\#P$ -hard or polynomial time computable.*

*Proof.* Let us consider the case first that  $A$  is not bipartite – the bipartite case follows by analogous reasoning. Assume that  $\text{EVAL}^{\text{pin}}(A, D)$  is not  $\#P$ -hard. Then Lemma 3.4 implies that there is an  $\omega$ -algebraic Hermitian matrix  $H$  and a family  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  of diagonal matrices which define an **(H–STD)** problem such that

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(H, \mathbf{D}). \quad (9)$$

Therefore  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  cannot be  $\#P$ -hard. By Theorem 3.5 the matrix  $H$  and the family  $\mathbf{D}$  thus satisfy conditions **(GC)**, **(R1)** through **(R5)** and the Affinity Condition **(AF)**. Hence by Theorem 3.8 the problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is polynomial time computable. Therefore, equation (9) implies that  $\text{EVAL}^{\text{pin}}(A, D)$  is also polynomial time computable.  $\square$

*Proof (of Theorem 1.2).* Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Assume first that  $A$  is not  $\omega$ -algebraic for some  $\omega \in \mathbb{N}$ , then the Arithmetical Structure Lemma 3.1 implies that there is some  $\omega \in \mathbb{N}$  and an  $\omega$ -algebraic matrix  $A'$  such that  $\text{EVAL}(A, D) \equiv \text{EVAL}(A', D)$ . We therefore assume for simplicity that  $A$  is  $\omega$ -algebraic. We have

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}(A, D) \quad (10)$$

by the Pinning Lemma 3.2. Let  $\mathcal{I}$  be a partition of  $[m]$  into subsets  $I \in \mathcal{I}$  such that each  $A_{II}$  is a component of  $A$ . The following is true for each  $I \in \mathcal{I}$ .

*Claim 1.* If  $\text{EVAL}^{\text{pin}}(A_{II}, D_{II})$  is #P-hard then  $\text{EVAL}(A, D)$  is #P-hard.

To see this, let  $G, \phi$  be the input to  $\text{EVAL}^{\text{pin}}(A_{II}, D_{II})$  for some  $I \in \mathcal{I}$ . We may assume that  $G$  is connected and  $\text{def}(\phi) \neq \emptyset$ . Therefore, we have  $Z_{A_{II}, D_{II}}(\phi, G) = Z_{A, D}(\phi, G)$  and thus  $\text{EVAL}^{\text{pin}}(A_{II}, D_{II}) \leq \text{EVAL}^{\text{pin}}(A, D)$ . By equation (10) this proves Claim 1. We further have, for all digraphs  $G$ ,

$$Z_{A, D}(G) = \sum_{I \in \mathcal{I}} Z_{A_{II}, D_{II}}(G).$$

This proves that  $\text{EVAL}(A, D)$  is polynomial time computable if for all  $I \in \mathcal{I}$  the problem  $\text{EVAL}(A_{II}, D_{II})$  is. By Lemma 3.9 we see that for each component  $A_{II}$  of  $A$  either the preconditions of Claim 1 are given or  $\text{EVAL}^{\text{pin}}(A_{II}, D_{II})$  is polynomial time computable. This finishes the proof.  $\square$

## 4 Basic Technical Results

In this section we will give proofs of many technical results we will need later on. Most importantly, we will prove the Arithmetical Structure Lemma 3.1 in Section 4.3 and the Pinning Lemma 3.2 in Section 4.4. The proofs of these results require a considerable amount of other tools which we will develop in the following.

### 4.1 General Principles

Most reductions which we will present here have to deal with arbitrary input digraphs  $G$  and pinnings  $\phi$ . To avoid tedious reasoning on trivial or vacuous cases we will introduce some *general principles* which we will apply whenever necessary.

**Lemma 4.1 (Connectedness Principle).** *Fix one of  $\text{EVAL}^{\text{pin}}(A, D)$ ,  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  or  $\text{EVAL}(A, D)$ . If we know how to solve the problem in polynomial time given that the input is restricted to connected digraphs, then the general problem can be solved in polynomial time.*

*Proof.* We give the proof for  $\text{EVAL}^{\text{pin}}(A, D)$ , the other cases are analogous. Let  $G = (V, E)$  be a given digraph with components  $G_1, \dots, G_c$ . Each pinning  $\phi$  of vertices of  $G$  to entries of  $A$  can be partitioned into pinnings (possibly empty)  $\phi_1, \dots, \phi_c$  corresponding to the vertices of the components of  $G$ . Then

$$Z_{A, D}(\phi, G) = \prod_{i=1}^c Z_{A, D}(\phi_i, G_i).$$

Since we know how to compute the values  $Z_{A, D}(\phi_i, G_i)$  in polynomial time, the value  $Z_{A, D}(\phi, G)$  can be computed by the above equation.  $\square$



**Lemma 4.2 (The Pinning Principle).** *Fix one of  $\text{EVAL}^{\text{pin}}(A, D)$  or  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$ . Assume that this problem can be solved in polynomial time if the input allows only non-trivial pinnings. Then the general problem can be solved in polynomial time.*

*Proof.* We give the proof for  $\text{EVAL}^{\text{pin}}(A, D)$ , the other cases are analogous. Assume that  $A$  is an  $m \times m$  matrix and let  $G, \phi$  be an instance of  $\text{EVAL}^{\text{pin}}(A, D)$ . If  $\text{def}(\phi) = \emptyset$ , fix an arbitrary vertex  $v \in V$  and let  $\phi_i$  for every  $i \in [m]$  be the mapping defined by  $v \mapsto i$ . We have

$$Z_{A,D}(G) = \sum_{i=1}^m D_{ii} \cdot Z_{A,D}(\phi_i, G).$$

Each value  $Z_{A,D}(\phi_i, G)$  can be computed in polynomial time.  $\square$

For  $A$  an  $m \times m$  matrix and  $\pi : [m] \rightarrow [m]$  a permutation, define  $A_{\pi\pi}$  by  $(A_{\pi\pi})_{ij} = A_{\pi(i)\pi(j)}$  for all  $i, j \in [m]$ . It is straightforward to see that simultaneous permutation of the rows and columns of  $A$  do not alter the partition function:

**Lemma 4.3 (Permutability Principle).** *Let  $A, D \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  and  $\pi : [m] \rightarrow [m]$  a permutation. Then  $\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(A_{\pi\pi}, D_{\pi\pi})$ . This holds analogously for congruential partition functions.*

## 4.2 Technical Lemmas

**Lemma 4.4.** *Let  $0 < x_1 < \dots < x_n$  be positive in  $\mathbb{R}_{\mathbb{A}}$ .  $c_1, \dots, c_n \in \mathbb{C}_{\mathbb{A}}$ . There is a  $p_0 \in \mathbb{N}$  such that for all  $p \geq p_0$ , the following equation holds if, and only if, all coefficients  $c_i$  are zero.*

$$0 = \sum_{i=1}^n c_i x_i^p. \quad (11)$$

Further  $p_0$  is computable from input  $x_1, \dots, x_n, c_1, \dots, c_n$ .

*Proof.* Note that, if  $0 = c_1 = \dots = c_n$ , then equation (11) is satisfied for all  $p \geq 0$ . Assume therefore that there is at least one non-zero  $c_i$ . We perform induction on the maximum index  $m \leq n$  such that  $c_m \neq 0$ . If  $m = 1$  then  $\sum_{i=1}^n c_i x_i^p = c_1 x_1^p$  and the proof follows for  $p_0 = 0$ . For  $m > 1$  note that

$$\left| \sum_{i=1}^n c_i x_i^p \right| \geq \left| c_m x_m^p - \sum_{i=1}^{m-1} c_i x_i^p \right|$$

and the right hand side is larger than zero, if  $|c_m| x_m^p > \sum_{i=1}^{m-1} |c_i| x_i^p$ . If all  $c_1, \dots, c_{m-1}$  are zero, we are done with  $p_0 = 0$  and let  $x = \max\{x_i \mid c_i \neq 0, i \in [m-1]\}$  otherwise. We see that equation (11) is not satisfied if

$$\left( \frac{x_m}{x} \right)^p > \sum_{i=1}^{m-1} \frac{|c_i|}{|c_m|}.$$

As  $x_m > x$  this inequality is satisfied for large enough  $p$ . We define  $p_0$  such that this holds.  $\square$

### 4.2.1 Twin Reduction.

Let  $A \in \mathbb{C}^{m \times m}$  be Hermitian. We say that two rows  $A_{i,*}$  and  $A_{j,*}$  are *twins*, if  $A_{i,*} = A_{j,*}$ . A matrix  $A$  is *twin-free* if it has no twins. Twins induce an equivalence relation on the rows of  $A$ . Let  $I_1, \dots, I_k$  be the equivalence classes of this relation. Since  $A$  is Hermitian these classes are also the equivalence classes of the twin relation on the columns of  $A$ . The *twin resolvent* of  $A$  is the  $k \times k$  matrix  $[A]$ , defined by

$$[A]_{i,j} = A_{\mu,\nu} \text{ for some } \mu \in I_i \text{ and } \nu \in I_j.$$

We say that  $[A]$  is obtained from  $A$  by *twin reduction*. The *twin resolution mapping*  $\tau : [m] \rightarrow [k]$  of  $A$  is defined such that  $\mu \in I_{\tau(\mu)}$  for all  $\mu \in [m]$ . Hence  $[A]_{\tau(i),\tau(j)} = A_{i,j}$  for all  $i, j \in [m]$ .

To use twin reductions in the context of partition functions, we need to consider their effect on the diagonal matrices  $D$  associated to  $A$ . We will see that the following diagonal  $k \times k$  matrix  $D^{[A]}$  captures this effect

$$D_{i,i}^{[A]} = \sum_{\nu \in I_i} D_{\nu,\nu} \text{ for all } i \in [k]. \quad (12)$$

Analogously, for a family  $\mathbf{D} = (D^{[c]})_{c \in \mathbb{Z}_\omega}$  of congruential vertex weights, we define a family  $\mathbf{D}^{[A]} = (D^{[A],[c]})_{c \in \mathbb{Z}_\omega}$  of diagonal  $k \times k$  matrices by

$$D_{i,i}^{[A],[c]} = \sum_{\nu \in I_i} D_{\nu,\nu}^{[c]} \text{ for all } i \in [k] \text{ and all } c \in \mathbb{Z}_\omega.$$

**Lemma 4.5 (Twin Reduction Lemma).** *Let  $A \in \mathbb{C}^{m \times m}$  be Hermitian. Let  $I_1, \dots, I_k$  be the equivalence classes of the twin relation on  $A$  and  $\tau$  be the twin resolution mapping of  $A$ . The following is true for all digraphs  $G$  and pinning  $\phi$ :*

(1) *Let  $\mathbf{D} = (D^{[c]})_{c \in \mathbb{Z}_\omega}$  a family of congruential vertex weights, then*

$$Z_{A,\mathbf{D}}(\phi, G) = Z_{[A],\mathbf{D}^{[A]}}(\tau \circ \phi, G).$$

(2) *Let  $D$  be a diagonal  $m \times m$  matrix of vertex weights. Then*

$$Z_{A,D}(\phi, G) = Z_{[A],D^{[A]}}(\tau \circ \phi, G).$$

*Proof.* Let us start by proving (1). For a digraph  $G = (V, E)$  and a pinning  $\phi$ , let  $V' = V \setminus \text{def}(\phi)$ . We have

$$\begin{aligned} Z_{A,\mathbf{D}}(\phi, G) &= \sum_{\phi \subseteq \sigma : V \rightarrow [m]} \prod_{uv \in E} A_{\sigma(u),\sigma(v)} \prod_{v \in V'} D_{\sigma(v),\sigma(v)}^{[\partial(v)]} \\ &= \sum_{\phi \subseteq \sigma : V \rightarrow [m]} \prod_{uv \in E} [A]_{\tau \circ \sigma(u), \tau \circ \sigma(v)} \prod_{v \in V'} D_{\sigma(v),\sigma(v)}^{[\partial(v)]} \end{aligned}$$

where the second equality follows from the definition of  $\tau$ . As for all configurations  $\sigma : V \rightarrow [m]$  we have  $\tau \circ \sigma : V \rightarrow [k]$ , we can partition the  $\sigma$  into classes according to their images

under concatenation with  $\tau$  and obtain:

$$\begin{aligned} Z_{A, \mathbf{D}}(\phi, G) &= \sum_{\sigma': V \rightarrow [k]} \sum_{\substack{\phi \subseteq \sigma: V \rightarrow [m] \\ \tau \circ \sigma = \sigma'}} \prod_{uv \in E} [A]_{\sigma'(u), \sigma'(v)} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} \\ &= \sum_{\tau \circ \phi \subseteq \sigma': V \rightarrow [k]} \prod_{uv \in E} [A]_{\sigma'(u), \sigma'(v)} \left( \sum_{\substack{\phi \subseteq \sigma: V \rightarrow [m] \\ \tau \circ \sigma = \sigma'}} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} \right) \end{aligned}$$

Fix some  $\sigma' : V \rightarrow [k]$ . For  $\sigma : V \rightarrow [m]$  we have  $\tau \circ \sigma = \sigma'$  if and only if  $\sigma'^{-1}(\{i\}) = \sigma^{-1}(I_i)$  for all  $i \in [k]$ . Define for all  $i \in [k]$  the set  $V_i := \sigma'^{-1}(\{i\})$  and the mapping  $\phi_i := \phi \upharpoonright_{\text{def}(\phi) \cap V_i}$ , then

$$\begin{aligned} \sum_{\substack{\phi \subseteq \sigma: V \rightarrow [m] \\ \tau \circ \sigma = \sigma'}} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} &= \sum_{\substack{\phi \subseteq \sigma: V \rightarrow [m] \\ \forall i \in [k]: \sigma(V_i) \subseteq I_i}} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} \\ &= \prod_{i=1}^k \sum_{\phi_i \subseteq \sigma_i: V_i \rightarrow I_i} \prod_{v \in V_i \setminus \text{def}(\phi_i)} D_{\sigma_i(v), \sigma_i(v)}^{\llbracket \partial(v) \rrbracket} \\ &= \prod_{i=1}^k \prod_{v \in V_i \setminus \text{def}(\phi_i)} \sum_{\nu \in I_i} D_{\nu, \nu}^{\llbracket \partial(v) \rrbracket} \\ &= \prod_{v \in V'} D_{\sigma'(v), \sigma'(v)}^{[A], \llbracket \partial(v) \rrbracket} \end{aligned}$$

Hence

$$Z_{A, \mathbf{D}}(\phi, G) = \sum_{\tau \circ \phi \subseteq \sigma': V \rightarrow [k]} \prod_{uv \in E} [A]_{\sigma'(u), \sigma'(v)} \prod_{v \in V'} D_{\sigma'(v), \sigma'(v)}^{[A], \llbracket \partial(v) \rrbracket} = Z_{[A], \mathbf{D}^{[A]}}(\tau \circ \phi, G).$$

For the proof of (2) notice that  $D^{\llbracket c \rrbracket} = D$  implies  $D^{[A], \llbracket c \rrbracket} = D^{[A]}$  for every  $c \in \mathbb{Z}_\omega$ . The claim hence follows by Lemma 2.1.  $\square$

**Corollary 4.6.** *We have  $\text{EVAL}^{\text{pin}}(A, \mathbf{D}) \equiv \text{EVAL}^{\text{pin}}([A], \mathbf{D}^{[A]})$ .*

#### 4.2.2 Root Of Unity Transfer

Lemma 4.7 explains a way to transfer certain values from the Hermitian matrix  $A \in \mathbb{C}^{m \times m}$  into the vertex weights of the partition function.

**Lemma 4.7 (Root Of Unity Transfer Lemma).** *Let  $A \in \mathbb{C}^{m \times m}$  be Hermitian and  $\omega$ -algebraic. Let  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  be a family of congruential vertex weights and let  $\Pi$  be a diagonal  $m \times m$  matrix whose diagonal entries are  $\omega$ -th roots of unity. Define  $A' = \Pi A \bar{\Pi}$  and a family of diagonal matrices  $\mathbf{D}' = (D'^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  by  $(D')^{\llbracket c \rrbracket} = \Pi^c D^{\llbracket c \rrbracket}$ .*

*There is a polynomial time computable function  $f_\Pi$  such that for every digraph  $G$  and pinning  $\phi$  we have.*

$$Z_{A, \mathbf{D}}(\phi, G) = f_\Pi(\phi) \cdot Z_{A', \mathbf{D}'}(\phi, G).$$

*Furthermore,  $f_\Pi$  is non-zero for all  $\phi$ .*

*Proof.* Let  $G = (V, E)$  be a given digraph and  $\phi$  a pinning. With  $V' = V \setminus \text{def}(\phi)$  we have

$$\begin{aligned}
Z_{A, \mathbf{D}}(\phi, G) &= \sum_{\substack{\sigma: V \rightarrow [m] \\ \sigma \supseteq \phi}} \prod_{uv \in E} A_{\sigma(u)\sigma(v)} \prod_{v \in V'} D_{\sigma(v)\sigma(v)}^{[\partial(v)]} \\
&= \sum_{\substack{\sigma: V \rightarrow [m] \\ \sigma \supseteq \phi}} \prod_{uv \in E} \Pi_{\sigma(u)\sigma(v)} A'_{\sigma(u)\sigma(v)} \bar{\Pi}_{\sigma(v)\sigma(v)} \prod_{v \in V'} D_{\sigma(v)\sigma(v)}^{[\partial(v)]} \\
&= \left( \prod_{v \in \text{def}(\phi)} \Pi_{\phi(v)\phi(v)}^{\partial(v)} \right) \sum_{\substack{\sigma: V \rightarrow [m] \\ \sigma \supseteq \phi}} \prod_{uv \in E} A'_{\sigma(u)\sigma(v)} \prod_{v \in V'} \Pi_{\sigma(v)\sigma(v)}^{\partial(v)} D_{\sigma(v)\sigma(v)}^{[\partial(v)]}
\end{aligned}$$

Now  $\Pi^{\partial(v)} = \Pi^{[\partial(v)]}$  as all diagonal entries of  $\Pi$  are  $\omega$ -th roots of unity. Therefore,

$$\begin{aligned}
Z_{A, \mathbf{D}}(\phi, G) &= \left( \prod_{v \in \text{def}(\phi)} \Pi_{\phi(v)\phi(v)}^{\partial(v)} \right) \sum_{\substack{\sigma: V \rightarrow [m] \\ \sigma \supseteq \phi}} \prod_{uv \in E} A'_{\sigma(u)\sigma(v)} \prod_{v \in V'} \Pi_{\sigma(v)\sigma(v)}^{[\partial(v)]} D_{\sigma(v)\sigma(v)}^{[\partial(v)]} \\
&= \left( \prod_{v \in \text{def}(\phi)} \Pi_{\phi(v)\phi(v)}^{\partial(v)} \right) \sum_{\substack{\sigma: V \rightarrow [m] \\ \sigma \supseteq \phi}} \prod_{uv \in E} A'_{\sigma(u)\sigma(v)} \prod_{v \in V'} (D')_{\sigma(v)\sigma(v)}^{[\partial(v)]} \\
&= \left( \prod_{v \in \text{def}(\phi)} \Pi_{\phi(v)\phi(v)}^{\partial(v)} \right) Z_{A', \mathbf{D}'}(\phi, G)
\end{aligned}$$

Note that the factor  $\left( \prod_{v \in \text{def}(\phi)} \Pi_{\phi(v)\phi(v)}^{\partial(v)} \right)$  is nonzero and polynomial time computable. In particular, this factor equals 1 if  $\text{def}(\phi) = \emptyset$ .  $\square$

The above lemma directly yields,

**Corollary 4.8.** *We have  $\text{EVAL}^{\text{pin}}(A, \mathbf{D}) \equiv \text{EVAL}^{\text{pin}}(A', \mathbf{D}')$ .*

### 4.3 The Arithmetical Structure Lemma

In this section we will give the proof of Lemma 3.1. We need some preparation.

**EVAL( $A, D$ ) and COUNT( $A, D$ ).** Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a matrix and  $G = (V, E)$  a digraph. We define a set of *potential weights*

$$\mathcal{W}_A(G) := \left\{ \prod_{i, j \in [m]} A_{ij}^{m_{ij}} \mid \sum_{i, j \in [m]} m_{ij} = |E|, \text{ and } m_{ij} \geq 0, \text{ for all } i, j \in [m] \right\}. \quad (13)$$

For some  $w \in \mathbb{C}_{\mathbb{A}}$  denote the set of configurations with weight  $w$  by

$$\mathcal{C}_A(G, w) := \left\{ \sigma : V \rightarrow [m] \mid w = \prod_{uv \in E} A_{\sigma(u)\sigma(v)} \right\}.$$

Define the value

$$N_{A,D}(G, w) := \sum_{\sigma \in C_A(G, w)} \prod_{v \in V} D_{\sigma(v)\sigma(v)}$$

$\text{COUNT}(A, D)$  denotes the problem of computing  $N_{A,D}(G, w)$  for some given digraph  $G = (V, E)$  and a weight  $w \in \mathbb{C}_A$ . We use an interpolation technique from [DG00]:

**Lemma 4.9.** *Let, for some fixed  $\theta \in \mathbb{C}_A$  let  $x_1, \dots, x_n \in \mathbb{Q}(\theta)$  be pairwise different and non-zero. Let  $b_1, \dots, b_n \in \mathbb{Q}(\theta)$  be arbitrary such that*

$$b_j = \sum_{i=1}^n c_i x_i^j \text{ for all } j \in [n].$$

*Then the coefficients  $c_1, \dots, c_n$  are uniquely determined and can be computed in polynomial time.*

**Lemma 4.10.** *For every matrix  $A \in \mathbb{C}_A^{m \times m}$  and  $D \in \mathbb{C}_A^{m \times m}$  we have*

$$\text{EVAL}(A, D) \equiv \text{COUNT}(A, D).$$

*Proof.* Let  $G = (V, E)$  be a digraph. We have

$$Z_{A,D}(G) = \sum_{w \in \mathcal{W}_A(G)} w \sum_{\sigma \in C_A(G, w)} \prod_{v \in V} D_{\sigma(v)\sigma(v)} = \sum_{w \in \mathcal{W}_A(G)} w \cdot N_{A,D}(G, w).$$

As the cardinality of  $\mathcal{W}_A(G)$  is polynomial in the size of  $G$  this proves  $\text{EVAL}(A, D) \leq \text{COUNT}(A, D)$ . For the backward direction let  $G^{(t)}$  denote the digraph obtained from  $G$  by replacing each edge with  $t$  copies of it. We have

$$Z_{A,D}(G^{(t)}) = \sum_{\sigma: V \rightarrow [m]} \left( \prod_{uv \in E} A_{\sigma(u)\sigma(v)} \right)^t \prod_{v \in V} D_{\sigma(v)\sigma(v)} = \sum_{w \in \mathcal{W}_A(G)} w^t \cdot N_{A,D}(G, w).$$

Using an  $\text{EVAL}(A, D)$  oracle, we can evaluate this for  $t = 1, \dots, |\mathcal{W}_A(G)|$ . Therefore the values  $N_{A,D}(G, w)$  can be recovered in polynomial time by Lemma 4.9.  $\square$

### 4.3.1 The Proof of Lemma 3.1

To measure the time needed to perform operations on algebraic numbers, we need to introduce their *description length*. For an integer  $a \in \mathbb{Z}$  let its *description length* be  $\text{len}(a) := \lceil \log_2 |a| \rceil + 2$ . For a rational number  $q = \frac{a}{b}$  with  $a, b \in \mathbb{Z}$  we define  $\text{len}(q) := \text{len}(a) + \text{len}(b)$ . For a vector  $\mathbf{a} \in \mathbb{Q}^n$  we define  $\text{len}(\mathbf{a}) = \text{len}(a_1) + \dots + \text{len}(a_n)$ . This defines the description lengths of algebraic numbers in  $\mathbb{Q}(\theta)$  in standard representation. The description length  $\text{len}(A)$  of a matrix  $A \in \mathbb{Q}^{n \times n}$  is the sum of the description lengths of its entries.

Let  $B = \{b_1, \dots, b_n\} \subseteq \mathbb{C}_A$  be a set of algebraic numbers. By  $\langle B \rangle$  we denote the *multiplicative span* of  $B$  that is  $\langle B \rangle = \{\zeta \cdot \prod_{b \in B} b^{\lambda_b} \mid \lambda_b \in \mathbb{Z}, \text{ for all } b \in B, \zeta \text{ is a root of unity}\}$ . The set  $B$  is called *multiplicatively independent*, if for all  $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$  the following holds: if  $b_1^{\lambda_1} \dots b_n^{\lambda_n}$  is a root of unity then  $\lambda_1 = \dots = \lambda_n = 0$ . In all other cases we say that  $B$  is *multiplicatively dependent*. We say that a set  $S$  is *effectively representable* in terms of  $B$ , if for given  $x \in S$  we can compute  $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$  such that  $x \cdot b_1^{\lambda_1} \dots b_n^{\lambda_n}$  is a root of unity. A set  $B$  is an *effective representation system* for a set  $S$ , if  $S$  is effectively representable in terms of  $B$  and  $B$  is multiplicatively independent. We need a result from [Ric01]:

**Lemma 4.11 (Theorem 2 in [Ric01]).** *Let  $a_1, \dots, a_n \in \mathbb{Q}(\theta)$  given in standard representation, each of description length at most  $s$ . There is a matrix  $A \in \mathbb{Z}^{n \times n}$  such that, for vectors  $\lambda \in \mathbb{Z}^n$  we have*

$$\prod_{i=1}^n a_i^{\lambda_i} \text{ is a root of unity, if, and only if, } A \cdot \lambda = 0. \quad (14)$$

*The description length of  $A$  is bounded by a computable function in  $n$  and  $s$ .*

This theorem has a straightforward algorithmic consequence.

**Corollary 4.12.** *Let  $a_1, \dots, a_n \in \mathbb{Q}(\theta)$  be given in standard representation. There is an algorithm which decides if there is a non-zero vector  $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$  such that*

$$\prod_{i=1}^n a_i^{\lambda_i} \text{ is a root of unity.} \quad (15)$$

*Furthermore, if it exists, the algorithm computes such a vector  $\lambda$ .*

**Lemma 4.13.** *Let  $B = \{b_1, \dots, b_n\} \subseteq \mathbb{C}_{\mathbb{A}}$  be a multiplicatively dependent set of algebraic numbers. Then there is a set  $B'$  such that  $|B'| < |B|$  and  $B$  is effectively representable by  $B'$ .*

*Proof.* Since  $B$  is multiplicatively dependent, Corollary 4.12 implies that we can compute a non-zero vector  $\lambda \in \mathbb{Z}^n$  such that  $b_1^{\lambda_1} \cdots b_n^{\lambda_n}$  is a root of unity. We can easily make sure that at least one of the  $\lambda_i$  is larger than zero. Assume therefore w.l.o.g. that  $\lambda_1 > 0$ . Fix a set  $B' = \{b'_2, \dots, b'_n\}$  where each  $b'_i$  is a  $\lambda_1$ -th root of  $b_i$ , that is  $(b'_i)^{\lambda_1} = b_i$ . Then

$$b_1^{\lambda_1} \cdot \left( \prod_{i=2}^n (b'_i)^{\lambda_i} \right)^{\lambda_1} \text{ is a root of unity and hence } b_n \cdot \prod_{i=0}^{n-1} (b'_i)^{\lambda_i} \text{ is a root of unity.}$$

All operations are computable and effective representation of  $B$  by  $B'$  follows.  $\square$

**Lemma 4.14.** *Let  $S \subseteq \mathbb{C}_{\mathbb{A}}$  be a set of algebraic numbers. There is an effective representation system  $B$  for  $S$  which can be computed effectively from  $S$ .*

*Proof.* Let  $B' = S$  and apply Lemma 4.13 recursively on  $B$ . Since the empty set is multiplicatively independent, after at most finitely many steps, we find an effective representation system  $B$  for  $S$ .  $\square$

*Proof (of Lemma 3.1).* Let  $S$  be the set of non-zero entries of  $A$ . By Lemma 4.14 we can compute an effective representation system  $B$  for  $S$ . However, with respect to our model of computation we need to be a bit careful, here: assume that  $S \subseteq \mathbb{Q}(\theta)$  for some primitive element  $\theta$ . The application of Lemma 4.14 does not allow us to stipulate that  $B \subseteq \mathbb{Q}(\theta)$ . But in another step of precomputation, we can compute another primitive element  $\theta'$  for the elements of  $B$  such that  $B \subseteq \mathbb{Q}(\theta')$ . Then we may consider all computations as taking place in  $\mathbb{Q}(\theta')$ .

Assume that  $B = \{b_1, \dots, b_n\}$ , then every non-zero entry of  $A$  has a unique computable representation

$$A_{ij} = \zeta_{ij} \cdot \prod_{\nu=1}^n b_{\nu}^{\lambda_{ij\nu}} \quad \text{for } \zeta_{ij} \text{ a root of unity.}$$

Let  $p_1, \dots, p_\beta$  be  $\beta = |B|$  distinct prime numbers and define  $A'$  as the matrix obtained from  $A$  by replacing in each non-zero entry  $A_{ij}$  the powers of  $b \in B$  by the corresponding powers of primes, that is,

$$A'_{ij} = \zeta_{ij} \cdot \prod_{\nu=1}^n p_\nu^{\lambda_{ij\nu}}.$$

Recall the definition of  $\mathcal{W}_A(G)$  in equation (13). For each  $w \in \mathcal{W}_A(G)$  we can, in polynomial time compute a representation  $w = \prod_{i,j} A_{ij}^{m_{ij}}$  as powers of elements in  $S$ . The effective representation of  $S$  in terms of  $B$  extends to  $\mathcal{W}_A(G)$  being effectively representable by  $B$ . Moreover, as  $S$  depends only on  $A$ , the representation of each  $w \in \mathcal{W}_A(G)$  is even polynomial time computable. We have

$$Z_{A,D}(G) = \sum_{w \in \mathcal{W}_A(G)} w \cdot N_{A,D}(G, w)$$

In particular, for each  $w \in \mathcal{W}_A(G)$ , we can compute unique  $\lambda_{w,1}, \dots, \lambda_{w,n} \in \mathbb{Z}$  such that  $w \cdot b_1^{\lambda_{w,1}} \dots b_n^{\lambda_{w,n}}$  is a root of unity. Define functions  $f$  and  $g$  such that for every  $w \in \mathcal{W}_A(G)$  we have

$$f(w) = \prod_{\nu=1}^n p_\nu^{\lambda_{w,\nu}} \quad \text{and} \quad g(w) = \prod_{\nu=1}^n b_\nu^{\lambda_{w,\nu}}.$$

Thus we obtain

$$Z_{A',D}(G) = \sum_{w \in \mathcal{W}_A(G)} w \cdot \frac{f(w)}{g(w)} \cdot N_{A,D}(G, w).$$

This yields a reduction for  $\text{EVAL}(A', D) \leq \text{EVAL}(A, D)$ . The other direction follows by

$$Z_{A,D}(G) = \sum_{w' \in \mathcal{W}_{A'}(G)} w' \cdot \frac{g(w')}{f(w')} \cdot N_{A',D}(G, w').$$

□

## 4.4 Pinning Vertices

In this section we will prove the Pinning Lemma 3.2. Before we can do this we need to establish an important property of partition functions  $Z_{A,D}$ : they allow to *reconstruct* the pair  $(A, D)$ , in the sense that the values  $Z_{A,D}(G)$  for all digraphs  $G$  determine the pair  $(A, D)$  up to isomorphism.

The notion of *isomorphism* employed here is given by considering  $A$  as (the adjacency matrix of) a weighted graph. Let  $A, D \in \mathbb{C}^{m \times m}$  and  $A', D' \in \mathbb{C}^{m' \times m'}$  be matrices such that  $D$  and  $D'$  are diagonal. Then  $A$  and  $A'$  are *isomorphic*, if  $m = m'$  and they admit a bijection  $\alpha : [m] \rightarrow [m']$  such that for all  $i, j \in [m]$  we have  $A_{ij} = A'_{\alpha(i), \alpha(j)}$ . We call  $\alpha$  an *isomorphism*. If further  $D_{ii} = D'_{\alpha(i), \alpha(i)}$  for all  $i \in [m]$  then the pairs  $(A, D)$  and  $(A', D')$  are *isomorphic*.

### 4.4.1 The Reconstruction Lemma

It will be convenient in the following to fix pinnings and consider digraphs compatible with these. To define this, fix  $\phi : [k] \rightarrow [m]$  to denote our pinning. A *k-labeled digraph*  $G$  is then a digraph with  $k$  distinct vertices labeled  $1, \dots, k$ , in this way  $\phi$  is compatible with every  $k$ -labeled digraph. The main technical result of this section, is the following.

**Lemma 4.15 (The Reconstruction Lemma).** *Let  $A \in \mathbb{C}^{m \times m}$  and  $A' \in \mathbb{C}^{m' \times m'}$  be twin-free,  $D \in \mathbb{R}^{m \times m}$  and  $D' \in \mathbb{R}^{m' \times m'}$  diagonal matrices of positive vertex weights and  $\phi : [k] \rightarrow [m]$  and  $\phi' : [k] \rightarrow [m']$  pinnings. Assume that*

$$Z_{A,D}(\phi, G) = Z_{A',D'}(\phi', G) \text{ for all } k\text{-labeled digraphs } G.$$

*Then there is an isomorphism  $\alpha$  between  $(A, D)$  and  $(A', D')$  such that  $\phi' = \phi \circ \alpha$ .*

Similar results been given first by Lovász [Lov67] for the case that  $A$  is the adjacency matrix of a graph and in [Lov06] for symmetric real-valued  $A$ . Schrijver [Sch09] gave a proof for symmetric complex-valued matrices.

We will prove Lemma 4.15 by extending the proof in [Lov06]. We will therefore fix  $m \geq m'$ , twin-free matrices  $A \in \mathbb{C}^{m \times m}$  and  $A' \in \mathbb{C}^{m' \times m'}$  and diagonal matrices  $D \in \mathbb{R}^{m \times m}$  and  $D' \in \mathbb{R}^{m' \times m'}$  of positive vertex weights. For convenience we will consider  $k$ -tuples  $\mathbf{x} \in [m]^k$  as pinnings  $\mathbf{x} : [k] \rightarrow [m]$  and for any  $x \in [m]$  the expression  $\mathbf{x}x$  then denotes a  $(k+1)$ -tuple with last component  $x$ . We define an equivalence relation between tuples  $\mathbf{x} \in [m]^k$  and  $\mathbf{y} \in [m']^k$  by

$$\mathbf{x} \sim \mathbf{y} \text{ iff } Z_{A,D}(\mathbf{x}, G) = Z_{A',D'}(\mathbf{y}, G) \text{ for all } k\text{-labeled digraphs } G.$$

The product  $G_1 G_2$  of two  $k$ -labeled digraphs is the digraph obtained from  $G_1$  and  $G_2$  by taking their disjoint union and identifying vertices with the same label. For  $k$ -labeled digraphs  $G_1$  and  $G_2$  and every  $\mathbf{x} \in [m]^k$  we have

$$Z_{A,D}(\mathbf{x}, G_1 G_2) = Z_{A,D}(\mathbf{x}, G_1) \cdot Z_{A,D}(\mathbf{x}, G_2). \quad (16)$$

**Lemma 4.16.** *Let  $\mathbf{x} \in [m]^k$  and  $\mathbf{y} \in [m']^k$  such that  $\mathbf{x} \sim \mathbf{y}$ . Then for every and  $x \in [m]$  there is a  $y \in [m']$  such that  $\mathbf{x}x \sim \mathbf{y}y$ .*

*Proof.* Note first that

$$Z_{A,D}(\mathbf{x}, G) = \sum_{x=1}^m D_{xx} Z_{A,D}(\mathbf{x}x, G).$$

The condition that  $\mathbf{x} \sim \mathbf{y}$  therefore implies that, for every  $(k+1)$ -labeled digraph  $G$

$$\sum_{x=1}^m D_{xx} Z_{A,D}(\mathbf{x}x, G) = \sum_{y=1}^{m'} D'_{yy} Z_{A',D'}(\mathbf{y}y, G). \quad (17)$$

Define pairs  $(X_1, Y_1), \dots, (X_s, Y_s)$  of sets in the following way. The sets  $X_1, \dots, X_s$  partition  $[m]$  with possibly some empty parts and  $Y_1, \dots, Y_s$  are partitions of  $[m']$  with possibly empty parts, as well. The partitions satisfy, for every  $i \in [s]$ , that  $x, x' \in X_i$  if, and only if,  $Z_{A,D}(\mathbf{x}x, G) = Z_{A,D}(\mathbf{x}x', G)$  for all  $k+1$ -labeled graphs  $G$ . The analogue holds for the  $y, y' \in Y_i$  with  $Z_{A',D'}(\mathbf{y}y, G) = Z_{A',D'}(\mathbf{y}y', G)$  for all  $k+1$ -labeled graphs  $G$ . Further for all  $i \in [s]$ , the set  $X_i \cup Y_i$  is non-empty and for all  $x \in X_i$  and  $y \in Y_i$  we have

$$Z_{A,D}(\mathbf{x}x, G) = Z_{A',D'}(\mathbf{y}y, G) \text{ for all } k+1\text{-labeled digraphs } G. \quad (18)$$

Define for all  $i \in [s]$  a  $(k+1)$ -tuple  $\mathbf{z}_i$  and a function  $Z(\mathbf{z}_i, G)$  such that  $\mathbf{z}_i := \mathbf{x}x$  for some  $x \in X_i$  and  $Z(\mathbf{z}_i, G) := Z_{A,D}(\mathbf{x}x, G)$  if  $X_i$  is non-empty and  $\mathbf{z}_i := \mathbf{y}y$  for  $y \in Y_i$  with  $Z(\mathbf{z}_i, G) := Z_{A',D'}(\mathbf{y}y, G)$  otherwise. Let furthermore

$$c_i := \sum_{x \in X_i} D_{xx} - \sum_{y \in Y_i} D'_{yy}$$



Equation (17) now simplifies to

$$0 = \sum_{i=1}^s c_i Z(\mathbf{z}_i, G).$$

We claim that  $c_i = 0$  for all  $i \in [s]$ . If this holds the proof of the lemma follows as by the non-negativity of the vertex weights  $c_i = 0$  implies  $X_i \neq \emptyset$  and  $Y_i \neq \emptyset$  which, by equation (18), provides us with the desired extensions of  $\mathbf{x}$  and  $\mathbf{y}$ . We will show, more generally, that for all sets  $I \subseteq [s]$  the equation

$$0 = \sum_{i \in I} c_i Z(\mathbf{z}_i, G) \quad \text{for all digraphs } G. \quad (19)$$

implies that  $c_i = 0$  for all  $i \in I$ . We will prove this by induction on the cardinality of  $I$ .

For  $I = \{i\}$  let  $E_{k+1}$  be the  $k+1$ -labeled digraph on  $k+1$  vertices which contains no edges. If  $\mathbf{z}_i = \mathbf{x}x$ , we have  $Z(\mathbf{z}_i, E_{k+1}) = Z_{A,D}(\mathbf{z}_i, E_{k+1}) = 1$  and thus equation (19) implies  $c_i = 0$ . An analogous argument proves the case that  $\mathbf{z}_i = \mathbf{y}y$ .

Let  $|I| > 1$ . By definition, for all  $i \neq j \in I$  there is a digraph  $G_{ij}$  such that  $Z(\mathbf{z}_i, G_{ij}) \neq Z(\mathbf{z}_j, G_{ij})$ . Partition  $I$  into equivalence classes  $J_0, \dots, J_t$  such that  $a, b \in J_\nu$  iff  $Z(\mathbf{z}_a, G_{ij}) = Z(\mathbf{z}_b, G_{ij})$ . Define, for each  $i \in [0, t]$  the tuple  $\mathbf{z}'_i$  such that  $\mathbf{z}'_i = \mathbf{z}_a$  for some  $a \in J_i$ . Let  $H^p$  denote the  $k+1$ -labelled graph product of  $H$  with itself taken  $p$  times, then by equation (16) and (19) we have

$$0 = \sum_{\nu=0}^t \left( \sum_{\mu \in J_\nu} c_\mu \right) Z(\mathbf{z}'_\nu, G_{ij}^p G) = \sum_{\nu=0}^t Z(\mathbf{z}'_\nu, G_{ij})^p \left( \sum_{\mu \in J_\nu} c_\mu Z(\mathbf{z}_\mu, G) \right).$$

By definition, the values  $Z(\mathbf{z}'_\nu, G_{ij})$  are pairwise different. It may be the case that one of these is zero. Assume w.l.o.g. that  $0 = Z(\mathbf{z}'_0, G_{ij})$ . For  $p = 1, \dots, t$ , this gives rise to a homogeneous system of linear equations with a Vandermonde determinant:

$$0 = \sum_{\nu=1}^t Z(\mathbf{z}'_\nu, G_{ij})^p \left( \sum_{\mu \in J_\nu} c_\mu Z(\mathbf{z}_\mu, G) \right).$$

Solving this system yields  $0 = \sum_{\mu \in J_\nu} c_\mu Z(\mathbf{z}_\mu, G)$  for all  $\nu \geq 1$ . Since  $|J_\nu| < n$ , the induction hypothesis implies that we have  $c_i = 0$  for all  $i \in J_\nu$  and every  $\nu \geq 1$ . Therefore, by equation (19), we further obtain

$$0 = \sum_{j \in J_0} c_j Z(\mathbf{z}_j, G).$$

which, again by the induction hypothesis, implies  $c_j = 0$  for all  $j \in J_0$ .  $\square$

**Lemma 4.17.** *Every map  $\psi : [m] \rightarrow [m']$  such that  $A_{ij} = A'_{\psi(i)\psi(j)}$  for all  $i, j \in [m]$  is injective.*

*Proof.* Let  $J$  be the image of  $\psi$  and define a mapping  $\psi' : J \rightarrow [m]$  such that for each  $j \in J$  we fix an  $i \in [m]$  with  $\psi(i) = j$  and define  $\psi'(j) = i$ . Define  $\phi : [m] \rightarrow [m]$  by  $\phi = \psi' \circ \psi$ .

The precondition of the lemma implies that  $A_{ij} = A_{\phi(i)\phi(j)}$  for all  $i, j \in [m]$ . We will show first that  $\phi$  has a power  $\phi^s$  which is *idempotent*, that is  $\phi^s = \phi^{2s}$ . To see this, note that by the finiteness of  $[m]$  not all powers of  $\phi$  can be different. Hence, there are  $l, k$  such that

$\phi^l = \phi^{l+k} = \phi^{l+ik}$  for all  $i \in \mathbb{N}$ . Multiplying from the left with  $\phi^j$  we have  $\phi^{l+j} = \phi^{l+j+ik}$  for all  $i, j \in \mathbb{N}$ . Let  $i$  be large enough such that  $ik - l > 0$  then with  $j = ik - l$  we have  $2(l+j) = l+j+ik$ . Hence  $\phi^{l+j} = \phi^{l+j+ik} = \phi^{2(l+j)}$ .

Now  $A_{ij} = A_{\phi(i)\phi(j)}$  implies  $A_{ij} = A_{\phi^s(i)\phi^s(j)}$  for all  $s$ . Hence for  $s$  such that  $\phi^s = \phi^{2s}$  we have

$$A_{ij} = A_{\phi^s(i)\phi^s(j)} = A_{\phi^{2s}(i)\phi^{2s}(j)} = A_{\phi^s(i)j} \text{ for all } j \in [m].$$

Recall that  $A$  is twin-free. Thus  $\phi^s$  is the identity and therefore  $\phi$  must be bijective. Further by the definition of  $\phi$  this implies that  $\psi$  is injective.  $\square$

**Lemma 4.18.** *Let  $\mathbf{x} \in [m]^m$  and  $\mathbf{y} \in [m']^m$  such that  $\mathbf{x}$  is bijective and  $\mathbf{x} \sim \mathbf{y}$ . Then there is an isomorphism  $\alpha$  between  $(A, D)$  and  $(A', D')$  such that  $\mathbf{y} = \alpha \circ \mathbf{x}$ .*

*Proof.* Define  $G_{ij}$  as the  $m$ -labeled digraph on  $m$  vertices with the single edge  $ij$ . Assume w.l.o.g. that  $x_i = i$  for all  $i \in [m]$ . By  $\mathbf{x} \sim \mathbf{y}$  we have

$$A_{ij} = Z_{A,D}(\mathbf{x}, G_{ij}) = Z_{A',D'}(\mathbf{y}, G_{ij}) = A'_{y_i y_j}. \quad (20)$$

Since  $A'$  is twin-free Lemma 4.17 implies that  $\mathbf{y}$  is injective and by the condition that  $m \geq m'$  it is thus bijective and  $m = m'$ . This gives rise to an isomorphism  $\alpha : [m] \rightarrow [m]$  between  $A$  and  $A'$  by defining  $\alpha(x_i) = \alpha(i) =: y_i$  for all  $i \in [m]$ .

It remains to show that  $D_{ii} = D'_{\alpha(i), \alpha(i)}$  holds for all  $i \in [m]$ . Let  $Q = \{i \in [m] \mid A_{i,*} \neq 0\}$  and  $P = \{j \in [m] \mid A_{*,j} \neq 0\}$  be the set of indices corresponding to non-zero rows and columns of  $A$ . If one of these sets is empty, then  $Q = P = \emptyset$  and  $A = (0)$  since  $A$  is twin-free and then the following claim implies  $D_{11} = D'_{11}$ .

*Claim 1.* We have

$$\sum_{j=1}^m D_{jj} = \sum_{j=1}^m D'_{\alpha(j)\alpha(j)}.$$

*Proof.* Let  $G_0$  be the  $m$ -labeled digraph on vertex set  $[m] \dot{\cup} \{v\}$  without edges. By  $\mathbf{x} \sim \mathbf{y}$  we have

$$\sum_{j=1}^m D_{jj} = Z_{A,D}(\mathbf{x}, G_0) = Z_{A',D'}(\mathbf{y}, G_0) = \sum_{j=1}^m D'_{\alpha(j)\alpha(j)}. \quad \dashv$$

Assume therefore that  $Q, P \neq \emptyset$ . Let  $p : Q \rightarrow \mathbb{N}$  be an mapping, we say that it is *non-vanishing* if there is an  $i \in Q$  such that  $p(i) > 0$ . Define  $G^{[p]}$  as the  $m$ -labeled digraph on vertex set  $[m] \dot{\cup} \{v\}$  with edges  $E = \{(iv)^{p(i)} \mid i \in Q\}$ , that is for each  $i \in Q$  there is an edge with multiplicity  $p(i)$ . Note in particular that the edge  $iv$  does not exist if  $p(i) = 0$ .

For every non-vanishing  $p : Q \rightarrow \mathbb{N}$ , we have

$$Z_{A,D}(\mathbf{x}, G^{[p]}) = \sum_{j \in P} D_{jj} \prod_{i \in Q} (A_{ij})^{p(i)}.$$

By  $\mathbf{x} \sim \mathbf{y}$  we have  $Z_{A,D}(\mathbf{x}, G^{[p]}) = Z_{A',D'}(\mathbf{y}, G^{[p]})$  and therefore,

$$\sum_{j \in P} D_{jj} \prod_{i \in Q} (A_{ij})^{p(i)} = \sum_{j \in P} D'_{\alpha(j)\alpha(j)} \prod_{i \in Q} (A'_{\alpha(i)\alpha(j)})^{p(i)}$$

Now  $\alpha$  is an isomorphism between  $A$  and  $A'$ , that is  $A_{ij} = A'_{\alpha(i)\alpha(j)}$  and thus the above simplifies to

$$0 = \sum_{j \in P} \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p(i)} \quad \text{for all non-vanishing } p : Q \rightarrow \mathbb{N}. \quad (21)$$

We shall show the following

*Claim 2.* Let  $J \subseteq P$  of cardinality at least 2 and assume that

$$0 = \sum_{j \in J} \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p(i)} \quad \text{for all non-vanishing } p : Q \rightarrow \mathbb{N}. \quad (22)$$

Then for every  $j \in J$ , there is a set  $J' \subset J$  with  $j \in J'$  such that

$$0 = \sum_{j \in J'} \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p(i)} \quad \text{for all non-vanishing } p : Q \rightarrow \mathbb{N}. \quad (23)$$

Before we prove this claim, let us see how it finishes the proof of the lemma. Its statement will be particularly true for  $J = P$  and the condition of which is given by equation (21). Thus, for every  $j \in P$  iterative application of this claim eventually implies

$$0 = \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p(i)} \quad \text{for all non-vanishing } p : Q \rightarrow \mathbb{N}.$$

Since  $j \in P$  there is an  $i \in Q$  such that  $A_{ij} \neq 0$ . Fix a  $p : Q \rightarrow \mathbb{N}$  which satisfies  $p(i) = 1$  and  $p(i') = 0$  for  $i' \neq i$ . Then we have  $0 = \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) A_{ij}$  and thus  $D_{jj} = D'_{\alpha(j)\alpha(j)}$ .

Therefore we obtain  $D_{jj} = D'_{\alpha(j)\alpha(j)}$  for all  $j \in P$ . If  $A$  contains no zero columns, we are done as then  $P = [m]$ . Otherwise, since  $A$  is twin-free, there is exactly one  $k$  such that  $A_{*,k} = 0$  and  $P \cup \{k\} = [m]$ . Thus Claim 1 further implies  $D_{kk} = D'_{\alpha(k)\alpha(k)}$ .

**The Proof of Claim 2.** As  $J$  is of cardinality at least 2, we may fix distinct  $j, j' \in J$ . By  $A$  being twin-free we may fix an  $i^* \in Q$  such that  $A_{i^*j} \neq A_{i^*j'}$ . Let  $p : Q \rightarrow \mathbb{N}$  be a non-vanishing mapping. Define a non-vanishing  $p_q : Q \rightarrow \mathbb{N}$  by  $p_q(i^*) = p(i^*) + q$  and  $p_q(i) = p(i)$  for all  $i \neq i^*$ . The condition of the claim implies that

$$\begin{aligned} 0 &= \sum_{j \in J} \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p_q(i)} \\ &= \sum_{j \in J} (A_{i^*j})^q \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p(i)} \end{aligned}$$

Partition  $J$  into equivalence classes  $J_0, \dots, J_t$  such that  $A_{i^*j} = A_{i^*j'}$  iff  $j, j' \in J_k$  for some  $k \in [t]$ . Define, for all  $k \in [0, t]$  values  $a_k := A_{i^*\nu}$  for some  $\nu \in J_k$ . Then

$$0 = \sum_{k=0}^t (a_k)^q \left( \sum_{j \in J_k} \left( D_{jj} - D'_{\alpha(j)\alpha(j)} \right) \prod_{i \in Q} (A_{ij})^{p(i)} \right)$$

It may be the case that one of the  $a_k$  values is zero. Assume w.l.o.g. that  $a_0 = 0$ . By condition, the above holds for all  $q$ . In particular, for  $q = 1, \dots, t$  this gives rise to a homogeneous system of linear equations

$$0 = \sum_{k=1}^t (a_k)^q \left( \sum_{j \in J_k} (D_{jj} - D'_{\alpha(j)\alpha(j)}) \prod_{i \in Q} (A_{ij})^{p(i)} \right).$$

Since all the values  $a_1, \dots, a_k$  are pairwise distinct and non-zero, this system has a Vandermonde determinant and is thus solvable, which implies, for all  $k \in [t]$ ,

$$0 = \sum_{j \in J_k} (D_{jj} - D'_{\alpha(j)\alpha(j)}) \prod_{i \in Q} (A_{ij})^{p(i)} \quad \text{for all non-vanishing } p : Q \rightarrow \mathbb{N}.$$

In combination with the condition (22) of the claim we also obtain

$$0 = \sum_{j \in J_0} (D_{jj} - D'_{\alpha(j)\alpha(j)}) \prod_{i \in Q} (A_{ij})^{p(i)} \quad \text{for all non-vanishing } p : Q \rightarrow \mathbb{N}.$$

Since the  $J_0, \dots, J_t$  are a partition of  $J$  and each of them has cardinality strictly smaller than  $J$ , the claim follows.  $\square$

Now we are able to prove the Reconstruction Lemma.

*Proof (of Lemma 4.15).* Let  $A, D$  be  $m \times m$  matrices and  $A', D'$  be  $m' \times m'$  matrices as given in the lemma and  $\phi, \phi'$  pinnings. In accordance with the notation of this section we define  $\mathbf{x} := \phi$  and  $\mathbf{y} := \phi'$  and we assume w.l.o.g. that  $m \geq m'$ . The precondition that  $Z_{A,D}(\phi, G) = Z_{A',D'}(\phi', G)$  for all digraphs  $G$  is tantamount to  $\mathbf{x} \sim \mathbf{y}$ .

It will be easier to work with surjective pinnings. Extend  $\mathbf{x}$  to a surjective  $\mathbf{x}' := \mathbf{x}\mathbf{z} \in [m]^l$  with  $l \geq m$ . Lemma 4.16 implies the existence of a  $\mathbf{z}'$  such that for  $\mathbf{y}' = \mathbf{y}\mathbf{z}'$  we have  $\mathbf{x}' \sim \mathbf{y}'$ . Observe that if we find an isomorphism  $\alpha$  between  $(A, D)$  and  $(A', D')$  such that  $\mathbf{y}' = \alpha \circ \mathbf{x}'$  then the proof follows as this implies  $\mathbf{y} = \alpha \circ \mathbf{x}$ .

We shall prove the existence of such an isomorphism. Assume w.l.o.g. that  $x'_i = i$  for all  $i \in [m]$  — we can achieve this by permuting the labels appropriately. Define  $\mathbf{x}'|_I = (x'_i)_{i \in I}$  for a set of indices  $I \subseteq [l]$ .

*Claim 1.* If  $\mathbf{x}''x \sim \mathbf{y}''y$  for some  $x \in [m]$  and  $y \in [m']$  then  $\mathbf{x}'' \sim \mathbf{y}''$ .

*Proof.* To see that this holds, assume the contrary. That is, for some  $k$ -labeled digraph  $G$  we have  $Z_{A,D}(\mathbf{x}'', G) \neq Z_{A',D'}(\mathbf{y}'', G)$ . Let  $G'$  be the digraph obtained from  $G$  by adding a single isolated vertex labeled  $k+1$ , then

$$Z_{A,D}(\mathbf{x}''x, G') = Z_{A,D}(\mathbf{x}'', G) \neq Z_{A',D'}(\mathbf{y}'', G) = Z_{A',D'}(\mathbf{y}''y, G')$$

contradicting the assumption.  $\dashv$

This claim implies that  $\mathbf{x}'|_{[m]} \sim \mathbf{y}'|_{[m]}$ . The  $m$ -tuple  $\mathbf{x}'|_{[m]}$  is bijective by definition. Lemma 4.18 thus implies  $\mathbf{y}'|_{[m]} = \alpha \circ \mathbf{x}'|_{[m]}$  for some isomorphism  $\alpha$  between  $(A, D)$  and  $(A', D')$ .

It remains to show that for all  $j \in [m+1, l]$  we have  $y'_j = \alpha(x'_j)$ . The bijectivity of  $\mathbf{x}'|_{[m]}$  implies  $x'_j = x'_r$  for an appropriate  $r \in [m]$ . Define  $I = \{1, \dots, r-1, r+1, \dots, m, j\}$ , then  $\mathbf{x}'|_I$  is bijective. Therefore, Lemma 4.18 implies the existence of an isomorphism  $\beta$  between  $(A, D)$  and  $(A', D')$  such that  $\mathbf{y}'|_I = \beta \circ \mathbf{x}'|_I$ , particularly implying bijectivity of  $\mathbf{y}'|_I$ . It follows thus for our original automorphism  $\alpha$  that  $y'_j = y'_r = \alpha(x'_r) = \alpha(x'_j)$ .  $\square$

#### 4.4.2 The Proof of The Pinning Lemma.

Applying the Reconstruction Lemma 4.15, we will now prove the Pinning Lemma.

**Lemma 4.19.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Let  $[A]$  be the twin resolvent of  $A$ . Then*

$$\text{EVAL}^{\text{pin}}([A], D^{[A]}) \equiv \text{EVAL}^{\text{pin}}(A, D) \quad \text{and} \quad \text{EVAL}([A], D^{[A]}) \equiv \text{EVAL}(A, D).$$

*Proof.* Let  $\tau$  be the twin resolution mapping on  $A$ . By the Twin Reduction Lemma 4.5(2) we have

$$Z_{A,D}(\phi, G) = Z_{[A],D^{[A]}}(\tau \circ \phi, G), \text{ for every digraph } G \text{ and pinning } \phi.$$

This yields  $\text{EVAL}^{\text{pin}}(A, D) \leq \text{EVAL}^{\text{pin}}([A], D^{[A]})$ . On the other hand, for some instance  $G$  and  $\phi'$  of  $\text{EVAL}^{\text{pin}}([A], D^{[A]})$  let  $\phi$  be a pinning on  $A$  such that  $\tau \circ \phi = \phi'$ , then the above also yields the backward direction. The result for  $\text{EVAL}(A, D)$  follows as the above holds likewise for empty pinnings.  $\square$

**Lemma 4.20.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  be a Hermitian and twin-free matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. Then*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}(A, D).$$

*Proof.* It suffices to show  $\text{EVAL}^{\text{pin}}(A, D) \leq \text{EVAL}(A, D)$  as the other direction holds trivially.

Let  $G = (V, E)$  and a pinning  $\phi$  be an instance of  $\text{EVAL}^{\text{pin}}(A, D)$ . By appropriate permutation of the rows/columns of  $A$  and  $D$  (cf. Lemma 4.3) we may assume that  $[k] = \text{img } \phi \subseteq [m]$  for some  $k \leq m$ . Let  $\hat{G} = (\hat{V}, \hat{E})$  be the graph obtained from  $G$  by collapsing the the sets  $\phi^{-1}(i)$  for all  $i \in [k]$ . Formally, define a map

$$\gamma(v) = \begin{cases} i & , v \in \phi^{-1}(i) \text{ for some } i \in [k] \\ v & , \text{ otherwise} \end{cases}$$

Then  $\hat{G}$  is a multi-digraph (with possibly some self-loops) defined by

$$\begin{aligned} \hat{V} &= [k] \dot{\cup} (V \setminus \text{def}(\phi)) \\ \hat{E} &= \{\gamma(u)\gamma(v) \mid uv \in E\}. \end{aligned}$$

Hence  $Z_{A,D}(\phi, G) = Z_{A,D}(\mathbf{id}_{[k]}, \hat{G})$  where  $\mathbf{id}_{[k]}$  denotes the identity map on  $[k]$ . Call two mappings  $\chi, \psi : [k] \rightarrow [m]$  *equivalent* if there is an automorphism  $\alpha$  of  $(A, D)$  such that  $\chi = \alpha \circ \psi$ . Partition the mappings  $\psi : [k] \rightarrow [m]$  into equivalence classes  $I_1, \dots, I_c$  according to this definition and for all  $i \in [c]$  fix some  $\psi_i \in I_i$ . Assume furthermore, that  $\psi_1 = \mathbf{id}_{[k]}$ . Clearly for any two  $\chi, \psi$  from the same equivalence class, we have  $Z_{A,D}(\chi, F) = Z_{A,D}(\psi, F)$  for every graph  $F$ . Therefore, for every graph  $G'$ ,

$$Z_{A,D}(G') = \sum_{i=1}^c Z_{A,D}(\psi_i, G') \cdot \left( \sum_{\psi \in I_i} \prod_{v \in \text{def}(\psi)} D_{\psi(v)\psi(v)} \right) \quad (24)$$

Define, for each  $i \in [c]$  the value  $c_i = \left( \sum_{\psi \in I_i} \prod_{v \in \text{def}(\psi)} D_{\psi(v)\psi(v)} \right)$ . We claim the following

*Claim 1.* Let  $I \subseteq [c]$  be a set of cardinality at least 2 such that  $1 \in I$ . Assume that we can, for every  $k$ -labeled digraph  $G'$ , compute the value

$$\sum_{i \in I} c_i \cdot Z_{A,D}(\psi_i, G'). \quad (25)$$

Then there is a proper subset  $I' \subset I$  which contains 1 such that we can compute, for every  $k$ -labeled digraph  $G''$ , the value

$$\sum_{i \in I'} c_i \cdot Z_{A,D}(\psi_i, G''). \quad (26)$$

This claim will allow us to finish the proof. To see this, note first that by equation (24) we can compute the value (25) for  $I = [c]$  and  $G' = \hat{G}$ . Thus after at most  $c$  iterations of Claim 1 we arrive at  $c_1 \cdot Z_{A,D}(\psi_1, \hat{G})$ . Further,  $c_1$  is effectively computable in time depending only on  $D$  and therefore we can compute  $Z_{A,D}(\mathbf{id}_{[k]}, \hat{G}) = Z_{A,D}(\phi, G)$ . This proves the reducibility  $\text{EVAL}^{\text{pin}}(A, D) \leq \text{EVAL}(A, D)$ .

**Proof Of Claim 1.** Assume that we can compute the value given in (25). Lemma 4.15 implies that for every pair  $i \neq j \in I$  there is a  $k$ -labeled digraph  $\Gamma$  such that

$$Z_{A,D}(\psi_i, \Gamma) \neq Z_{A,D}(\psi_j, \Gamma). \quad (27)$$

Fix such a pair  $i \neq j \in I$  and a graph  $\Gamma$  satisfying this equation. Note that this graph can be computed effectively in time depending only on  $A, D$  and  $\psi_i, \psi_j$ . Let  $G^s$  denote the digraph obtained from  $G$  by iterating  $s$  times the  $k$ -labeled product of  $G$  with itself. We can thus compute

$$\sum_{i \in I} c_i \cdot Z_{A,D}(\psi_i, G^s \Gamma) = \sum_{i \in I} c_i Z_{A,D}(\psi_i, G^s) \cdot Z_{A,D}(\psi_i, \Gamma)^s. \quad (28)$$

Partition  $I$  into classes  $J_0, \dots, J_z$  such that for every  $\nu \in [0, z]$  we have  $i', j' \in J_\nu$  if, and only if,  $Z_{A,D}(\psi_{i'}, \Gamma) = Z_{A,D}(\psi_{j'}, \Gamma)$ . Since one of these sets  $J_\nu$  contains 1 and all of these are proper subsets of  $I$ , it remains to show that we can compute, for each  $\nu \in [0, z]$ , the value

$$\sum_{i' \in J_\nu} c_{i'} Z_{A,D}(\psi_{i'}, G').$$

To prove this, define  $x_\nu := Z_{A,D}(\psi_{i'}, \Gamma)$  for each  $\nu \in [z]$  and an  $i' \in J_\nu$ . Equation (28) implies that we can compute

$$\sum_{\nu=0}^z x_\nu^s \left( \sum_{i' \in J_\nu} c_{i'} Z_{A,D}(\psi_{i'}, G') \right).$$

One of the values  $x_\nu$  might be zero. Assume therefore w.l.o.g. that  $x_0 = 0$ , then evaluating the above for  $s = 1, \dots, z$  yields a system of linear equations, which by Lemma 4.9 can be solved in polynomial time such that we can recover the values  $\sum_{i' \in J_\nu} c_{i'} Z_{A,D}(\psi_{i'}, G')$  for each  $\nu \geq 1$ . Using equation (25) we can thus also compute the value

$$\left( \sum_{i \in I} c_i \cdot Z_{A,D}(\psi_i, G') \right) - \sum_{\nu=1}^z \left( \sum_{i' \in J_\nu} c_{i'} Z_{A,D}(\psi_{i'}, G') \right) = \sum_{i' \in J_0} c_{i'} Z_{A,D}(\psi_{i'}, G').$$

□

*Proof (of the Pinning Lemma 3.2).* Fix the twin resolvent  $A' = [A]$  of  $A$  and let  $D' = D^{[A]}$ . By Lemma 4.20 we have  $\text{EVAL}^{\text{pin}}(A', D') \equiv \text{EVAL}(A', D')$ . Hence together with Lemma 4.19 we obtain the chain of reductions

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(A', D') \equiv \text{EVAL}(A', D') \equiv \text{EVAL}(A, D). \quad \square$$

## 4.5 Basic Complexity Results for Congruential Partition Functions

**A Basic Polynomial Time Case.** We provide the following basic tractability result which is a straightforward extension of Theorem 6 in [BG05].

**Lemma 4.21.** *Let  $A \in \mathbb{C}^{m \times m}$  be a Hermitian matrix and  $\mathbf{D}$  a family of diagonal matrices of vertex-weights. If  $A$  has rank 1 then  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is polynomial time computable.*

*Proof.* Let  $G = (V, E)$  be a given digraph and  $\phi$  a pinning. Let  $V' = V \setminus \text{def}(\phi)$  then

$$Z_{A, \mathbf{D}}(\phi, G) = \sum_{\phi \subseteq \sigma: V \rightarrow [m]} \prod_{uv \in E} A_{\sigma(u), \sigma(v)} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket}$$

As  $\text{rank } A = 1$ , there are vectors  $\mathbf{a}, \mathbf{b} \in \mathbb{C}_{\mathbb{A}}^m$  such that  $A = \mathbf{a}\mathbf{b}^T$ . Then, for every configuration  $\sigma : V \rightarrow [m]$ ,

$$\prod_{uv \in E} A_{\sigma(u), \sigma(v)} = \prod_{uv \in E} a_{\sigma(u)} b_{\sigma(v)} = \prod_{v \in V} a_{\sigma(v)}^{\deg^+(v)} b_{\sigma(v)}^{\deg^-(v)}.$$

Therefore,

$$\begin{aligned} Z_{A, D}(\phi, G) &= \sum_{\phi \subseteq \sigma: V \rightarrow [m]} \prod_{uv \in E} A_{\sigma(u), \sigma(v)} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} \\ &= \left( \prod_{v \in \text{def}(\phi)} a_{\phi(v)}^{\deg^+(v)} b_{\phi(v)}^{\deg^-(v)} \right) \sum_{\sigma: V' \rightarrow [m]} \prod_{v \in V'} a_{\sigma(v)}^{\deg^+(v)} b_{\sigma(v)}^{\deg^-(v)} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} \\ &= \prod_{v \in \text{def}(\phi)} a_{\phi(v)}^{\deg^+(v)} b_{\phi(v)}^{\deg^-(v)} \prod_{v \in V'} \sum_{i=1}^m a_i^{\deg^+(v)} b_i^{\deg^-(v)} D_{i, i}^{\llbracket \partial(v) \rrbracket} \end{aligned}$$

And the term in the last line can be evaluated in polynomial time.  $\square$

**Basic #P-hardness Results.** We need the following extension of the #P-hardness criterion of Theorem 1.1.

**Lemma 4.22.** *Let  $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  be a non-negative symmetric matrix and  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  a diagonal matrix of positive vertex weights. If  $A$  contains a block of rank at least 2 then  $\text{EVAL}(A, D)$  is #P-hard.*

We will give the proof of this Lemma below. From this result we derive a basic #P-hardness criterion for congruential partition functions.

**Lemma 4.23.** *Let  $A$  be a Hermitian matrix and  $\mathbf{D} = (D^{[c]})_{c \in \mathbb{Z}_\omega}$  such that  $D^{[0]}$  is a diagonal matrix of positive vertex weights. If  $\text{abs}(A)$  contains a block of row rank at least 2 then  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is #P-hard.*

*Proof.* Note first, that we have  $\text{EVAL}^{\text{pin}}(\text{abs}(A)^{(2)}, D^{\llbracket 0 \rrbracket}) \leq \text{EVAL}^{\text{pin}}(A, \mathbf{D})$ . To see this, let a graph  $G = (V, E)$  and a pinning  $\phi$  be an instance of  $\text{EVAL}^{\text{pin}}(\text{abs}(A), D^{\llbracket 0 \rrbracket})$ . Let  $G'$  be the graph obtained from  $G$  by adding for each existing arc  $uv$  an arc  $vu$ , we have  $Z_{\text{abs}(A)^{(2)}, D^{\llbracket 0 \rrbracket}}(\phi, G) = Z_{A, \mathbf{D}}(\phi, G')$ .

As  $\text{abs}(A)$  contains a block of row rank at least 2 the matrix  $\text{abs}(A)^{(2)}$  does so as well. By Lemma 4.22 the problem  $\text{EVAL}^{\text{pin}}(\text{abs}(A)^{(2)}, D^{\llbracket 0 \rrbracket})$  is #P-hard.  $\square$

**The proof of Lemma 4.22** The proof follows from Theorem 1.1 and the following Lemma which is a straightforward extension of Theorem 3.2 in [DG00]:

**Lemma 4.24.** *Let  $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  be a symmetric matrix with non-negative entries such that every pair of rows in  $A$  is linearly independent. Let  $D \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  be a diagonal matrix of positive vertex weights. Then*

$$\text{EVAL}(A) \leq \text{EVAL}(A, D).$$

The proof adapts the one in [DG00]; we present it for completeness. The following lemmas are restatements of those in [DG00] (see Lemma 3.4, 3.6, 3.7 and Theorem 3.1).

**Lemma 4.25.** *Let  $A \in \mathbb{R}_{\mathbb{A}}^{m \times m}$  be symmetric and non-singular,  $G = (V, E)$  a graph and  $F \subseteq E$ . If we know the values*

$$f_r(G) = \sum_{\sigma: V \rightarrow [m]} c_A(\sigma) \prod_{uv \in F} A_{\sigma(u)\sigma(v)}^r \quad (29)$$

*for all  $r \in [(|F| + 1)^{m^2}]$ , where  $c_A$  is a function depending on  $A$  but not on  $r$ . Then we can evaluate*

$$\sum_{\sigma: V \rightarrow [m]} c_A(\sigma) \prod_{uv \in F} (I_m)_{\sigma(u)\sigma(v)} \quad (30)$$

*in polynomial time.*

*Proof.* As  $A$  is symmetric and non-singular, there is an orthogonal matrix  $P$  such that  $P^T A P =: D$  is a diagonal matrix with non-zero diagonal. Every entry of  $A^r$  satisfies  $A_{ij}^r = (P D^r P^T)_{ij} = \sum_{\mu=1}^m P_{\sigma(u)\mu} P_{\sigma(v)\mu} (D_{\mu\mu})^r$ . By equation (29)

$$f_r(G) = \sum_{\sigma: V \rightarrow [m]} c_A(\sigma) \prod_{uv \in F} \sum_{\mu=1}^m P_{\sigma(u)\mu} P_{\sigma(v)\mu} (D_{\mu\mu})^r$$

Define  $\mathcal{W} = \{\prod_{i=1}^m (D_{ii})^{\alpha_i} \mid 0 \leq \alpha_i \text{ for all } i \in [m], \sum_{i=1}^m \alpha_i = |F|\}$  which can be constructed in polynomial time. We rewrite

$$f_r(G) = \sum_{w \in \mathcal{W}} c_w w^r.$$

for unknown coefficients  $c_w$ . By interpolation (cf. Lemma 4.9), we can recover these coefficients in polynomial time and can thus calculate  $f_0(G) = \sum_{w \in \mathcal{W}} c_w$ . We have

$$f_0(G) = \sum_{\sigma: V \rightarrow [m]} c_A(\sigma) \prod_{uv \in F} \sum_{\mu=1}^m P_{\sigma(u)\mu} P_{\sigma(v)\mu} (D_{\mu\mu})^0$$

which is equal to (30) by inspection.  $\square$



**Lemma 4.26.** *Let  $A \in \mathbb{R}^{m \times m}$  be a symmetric matrix in which every pair of distinct rows is linearly independent. Let  $D \in \mathbb{R}^{m \times m}$  be a diagonal matrix of non-negative vertex weights. Then every pair of rows in  $ADA$  is linearly independent. Furthermore there is an  $0 < \epsilon < 1$  such that*

$$|(ADA)_{ij}| \leq \epsilon \sqrt{(ADA)_{ii}(ADA)_{jj}}$$

*Proof.* Define  $Q = AD^{(1/2)}$ . We have  $ADA = AD^{(1/2)}D^{(1/2)}A^T = QQ^T$ . That is  $(ADA)_{ij} = \langle Q_{i,*}, Q_{j,*} \rangle$  every pair of rows in  $Q$  is linearly independent as it is linearly independent in  $A$ . By Cauchy-Schwarz  $\langle Q_{i,*}, Q_{j,*} \rangle < \sqrt{\langle Q_{i,*}, Q_{i,*} \rangle \langle Q_{j,*}, Q_{j,*} \rangle}$ , which implies that the corresponding  $2 \times 2$  submatrix of  $ADA$  defined by  $i$  and  $j$  has non-zero determinant. The existence of  $\epsilon$  follows.  $\square$

**Lemma 4.27.** *Let  $A \in \mathbb{R}^{m \times m}$  be a symmetric non-negative matrix in which every pair of distinct rows is linearly independent. Let  $D \in \mathbb{R}^{m \times m}$  be a diagonal matrix of positive vertex weights. Then there is a  $p \in \mathbb{N}$  such that the matrix  $(ADA)^{(p)}$  is non-singular.*

*Proof.* Let  $A' = ADA$  and consider the determinant

$$\det(A') = \sum_{\pi \in S_m} \pm \prod_{i=1}^m A'_{i\pi(i)}.$$

Let  $S_m$  be the set of permutations  $\pi : [m] \rightarrow [m]$ . For some  $\pi \in S_m$  define  $t(\pi) = |\{i \mid \pi(i) \neq i\}|$ . Let  $\epsilon$  be as in Lemma 4.26. Then

$$\prod_{i=1}^m |A'_{i\pi(i)}| \leq \epsilon^{t(\pi)} \prod_{i=1}^m \sqrt{A'_{ii}} \prod_{i=1}^m \sqrt{A'_{\pi(i)\pi(i)}} = \epsilon^{t(\pi)} \prod_{i=1}^m A'_{ii}. \quad (31)$$

Let  $\text{id}$  denote the trivial permutation. Then

$$\det((A')^{(p)}) \geq \left( \prod_{i=1}^m A'_{ii} \right)^p - \sum_{\pi \in S_m \setminus \{\text{id}\}} \left( \prod_{i=1}^m A'_{i\pi(i)} \right)^p.$$

By equation (31), we have

$$m! \epsilon^p \left( \prod_{i=1}^m A'_{ii} \right)^p \geq \sum_{\pi \in S_m \setminus \{\text{id}\}} \left( \prod_{i=1}^m A'_{i\pi(i)} \right)^p$$

and hence, as  $0 < \epsilon < 1$ , the matrix  $(ADA)^{(p)}$  is non-singular for large enough  $p$ .  $\square$

*Proof (of Lemma 4.24).* Fix a  $p \in \mathbb{N}$  such that  $(ADA)^{(p)}$  is non-singular by Lemma 4.27. Let a graph  $G = (V, E)$  be an instance of  $\text{EVAL}(A)$ . Define a graph  $G' = (V', E')$  by  $V' = \{v_0, \dots, v_{d-1} \mid v \in V, d = d_G(v)\}$  and  $E' = E'' \cup E'''$  for sets  $E'', E'''$  to be defined next. Let  $E'''$  be the set which contains, for each  $v \in V$  the cycle on  $\{v_0, \dots, v_{d_G(v)-1}\}$ , i.e.  $\{v_0 v_1, \dots, v_{d_G(v)-1} v_0\} \subseteq E'''$ . Let  $E''$  be the set of edges, such that each edge from  $E$  incident with  $v$  is connected to exactly one of the  $v_i$ .

We further construct a graph  $G'_{p,r}$  from  $G'$  as follows. Let  $T_p$  be a graph which consists  $p$  many length 2 paths connecting terminals  $a$  and  $b$ . Let  $T_{p,r}$  be the series composition of

$r$  many copies of  $T_p$ .  $G'_{p,r}$  is obtained from  $G'$  by replacing each edge in  $E'''$  with a distinct copy of  $T_{p,r}$ . We call  $a$  and  $b$  the "start" and "end" vertex of  $T_p$  and  $T_{p,r}$  has start and end vertices induced by the start and end vertices of the series composition of  $T_p$ .

For a graph  $H$  with designated "start" and "end" vertex let  $Z_{A,D}(i, j; H) := Z_{A,D}(\phi, H)$  such that  $\phi$  pins the start vertex to  $i$  and the end vertex to  $j$ .

*Claim 1.* Let  $C = (ADA)^{(p)}$ , then with  $X = D^{(1/2)}$ , we have for all  $i, j \in [m]$  and  $r \in \mathbb{N}$ ,

$$Z_{A,D}(i, j; T_{p,r}) = (X_{ii}X_{jj})^{-1}(XCX)_{ij}^r. \quad (32)$$

*Proof.* Straightforwardly,

$$Z_{A,D}(i, j; T_p) = \left( \sum_{k=1}^m A_{ik}A_{kj}D_{kk} \right)^p = (ADA)_{ij}^{(p)} = C_{ij}$$

and therefore

$$\begin{aligned} Z_{A,D}(i, j; T_{p,r}) &= \sum_{\substack{\sigma: [r+1] \rightarrow [m] \\ \sigma(1)=i, \sigma(r+1)=j}} \prod_{k=1}^r Z_{A,D}(\sigma(k), \sigma(k+1); T_p) \prod_{k=2}^r D_{\sigma(k), \sigma(k)} \\ &= (X_{ii}X_{jj})^{-1} \sum_{\substack{\sigma: [r+1] \rightarrow [m] \\ \sigma(1)=i, \sigma(r+1)=j}} \prod_{k=1}^r X_{\sigma(k), \sigma(k)} C_{\sigma(k), \sigma(k+1)} X_{\sigma(k+1), \sigma(k+1)} \end{aligned}$$

By inspection, the last line equals the right hand side of equation (32) — as claimed.  $\dashv$

For convenience, we count the indices of the vertices  $v_0, \dots, v_{d_G(v)-1}$  modulo  $d_G(v)$ . Particularly,  $v_{d_G(v)} = v_0$  and we have, for all  $r \in \mathbb{N}$ ,

$$Z_{A,D}(G'_{p,r}) = \sum_{\sigma: V' \rightarrow [m]} \prod_{uv \in E''} A_{\sigma(u)\sigma(v)} \prod_{v \in V'} D_{\sigma(v), \sigma(v)} \prod_{v \in V} \prod_{i=0}^{d_G(v)-1} Z_{A,D}(\sigma(v_i), \sigma(v_{i+1}); T_{p,r}).$$

As the vertices in  $V'$  are grouped according to the vertices in  $V$  we have

$$\prod_{v \in V'} D_{\sigma(v), \sigma(v)} = \prod_{v \in V} \prod_{i=0}^{d_G(v)-1} D_{\sigma(v_i), \sigma(v_i)}.$$

By (32), the expression  $\prod_{v \in V'} D_{\sigma(v), \sigma(v)} \prod_{v \in V} \prod_{i=0}^{d_G(v)-1} Z_{A,D}(\sigma(v_i), \sigma(v_{i+1}); T_{p,r})$  equals

$$\prod_{v \in V} \prod_{i=0}^{d_G(v)-1} D_{\sigma(v_i), \sigma(v_i)} \frac{(XCX)_{\sigma(v_i), \sigma(v_{i+1})}^r}{X_{\sigma(v_i), \sigma(v_i)} X_{\sigma(v_{i+1}), \sigma(v_{i+1})}} = \prod_{v \in V} \prod_{i=0}^{d_G(v)-1} (XCX)_{\sigma(v_i), \sigma(v_{i+1})}^r$$

Thus

$$Z_{A,D}(G'_{p,r}) = \sum_{\sigma: V' \rightarrow [m]} \prod_{uv \in E''} A_{\sigma(u)\sigma(v)} \prod_{uv \in E''} (XCX)_{\sigma(u)\sigma(v)}^r$$

Given the  $\text{EVAL}(A, D)$  oracle, we can, in polynomial time, evaluate this expression for every  $r$  which is polynomial in the size of  $G$ . Lemma 4.25 implies that we can compute the value

$$Z = \sum_{\sigma: V' \rightarrow [m]} \prod_{uv \in E''} A_{\sigma(u)\sigma(v)} \prod_{uv \in E'''} I_{\sigma(u)\sigma(v)}$$

It remains to show that  $Z = Z_A(G)$ . To see this, note that, for every configuration  $\sigma : V' \rightarrow [m]$  the weight  $\prod_{uv \in E''} A_{\sigma(u)\sigma(v)} \prod_{uv \in E'''} I_{\sigma(u)\sigma(v)}$  in the above expression is zero unless the following holds: For all  $v \in V$  we have  $\sigma(v_0) = \dots = \sigma(v_{d-1})$  for  $d = d_G(v)$ . For such a configuration, define  $\sigma' : V \rightarrow [m]$  by  $\sigma'(v) = \sigma(v_0)$  for every  $v \in V$ . Then

$$\prod_{uv \in E''} A_{\sigma(u), \sigma(v)} = \prod_{uv \in E} A_{\sigma'(u), \sigma'(v)}.$$

Since every configuration  $\sigma' : V \rightarrow [m]$  arises this way this finishes the proof.  $\square$

## 5 Connected Hermitian Matrices

In this section we will prove Lemma 3.4. To do this we will split the proof into two parts — one for the non-bipartite case and one for the bipartite case. The following two lemmas provide these two parts.

**Lemma 5.1 (The Non-Bipartite Case).** *Let  $A$  be a connected non-bipartite  $\omega$ -algebraic and Hermitian matrix and  $D$  a diagonal matrix of positive vertex weights. Then either the problem  $\text{EVAL}^{\text{pin}}(A, D)$  is  $\#P$ -hard or the following holds.*

*There is an  $\omega$ -algebraic Hermitian matrix  $H$  and a family  $\mathbf{U} = (U^{\mathbb{C}})_{c \in \mathbb{Z}_\omega}$  of diagonal matrices which define an **(H-STD)** problem such that*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(H, \mathbf{U}).$$

**Lemma 5.2 (The Bipartite Case).** *Let  $A$  be a connected bipartite  $\omega$ -algebraic Hermitian matrix and  $D$  a diagonal matrix of positive vertex weights. Then either  $\text{EVAL}^{\text{pin}}(A, D)$  is  $\#P$ -hard or the following holds.*

*There is an  $\omega$ -algebraic Hermitian matrix  $A'$  and a family  $\mathbf{U} = (U^{\mathbb{C}})_{c \in \mathbb{Z}_\omega}$  of diagonal matrices which define a **(B-H-STD)** problem such that*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(A', \mathbf{U}).$$

The proof of Lemma 3.4 follows directly from these two lemmas. In the remainder of this section we will give the proof of the Non-Bipartite Case Lemma 5.1. The proof of the Bipartite Case Lemma 5.2 is conceptually very similar, therefore we omit it, the full proof can be found in [Thu09].

**The proof of Lemma 5.1.** The strategy is to filter the problems  $\text{EVAL}^{\text{pin}}(A, D)$  until we are left with only those for which we can find a polynomial time equivalent **(H-STD)** problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{U})$ . This process of filtering will be performed by transforming in several steps the problem  $\text{EVAL}^{\text{pin}}(A, D)$  into a problem  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  where the matrix  $C$  and the family  $\mathbf{D}$  satisfy certain conditions, which will be given below. In each step, if a transformation is not possible, it will be shown that this implies  $\#P$ -hardness of the corresponding problem.

A bit of preparation is necessary. We say that a family  $\mathbf{D} = (D^{[\mathbb{c}]})_{c \in \mathbb{Z}_\omega}$  fits a matrix  $C$  if the dimensions of each  $D^{[\mathbb{c}]}$  match those of  $C$ . The matrix  $C$  under consideration will have a tensor product structure  $X \otimes H$ . Recall that we index the entries of such a matrix by pairs  $(\mu, i), (\nu, j)$  such that  $C_{(\mu, i), (\nu, j)} = X_{\mu\nu} \cdot H_{i,j}$ . The diagonal matrices  $(D^{[\mathbb{c}]})_{c \in \mathbb{Z}_\omega}$  fit  $C$  and therefore we index these in the same way. For convenience, we will alter the notation of the indices of these diagonal matrices a bit and let

$$D_{k,k}^{[\mathbb{c}];\kappa} := D_{(\kappa,k),(\kappa,k)}^{[\mathbb{c}]} \text{ for all } c \in \mathbb{Z}_\omega.$$

**Shape Conditions.** Let  $C$  be an  $\omega$ -algebraic Hermitian matrix and  $\mathbf{D} = (D^{[\mathbb{c}]})_{c \in \mathbb{Z}_\omega}$  a family of diagonal matrices of vertex weights that fits  $C$ . We define conditions on the shape of  $C$  and  $\mathbf{D}$ , two of which determine the shape of  $C$ .

- (C1) There are  $r, m \in \mathbb{N}$ ,  $\varsigma \in \{-1, 1\}$ , a non-singular normalized matrix  $H \in \mathbb{U}_\omega^{r \times r}$  and positive vectors  $v, w \in \mathbb{R}_\mathbb{A}^m$  such that  $v_1 < \dots < v_m$  and  $w$  depends linearly on  $v$  and

$$C = \varsigma \cdot vw^T \otimes H = \begin{pmatrix} \varsigma \cdot v_1 w_1 H & \dots & \varsigma \cdot v_1 w_m H \\ \vdots & \ddots & \vdots \\ \varsigma \cdot v_m w_1 H & \dots & \varsigma \cdot v_m w_m H \end{pmatrix}.$$

The submatrices  $C_{(\mu,*)(\nu,*)} = \varsigma \cdot v_\mu w_\nu H$  are the *tiles* of  $C$ .

- (C2) The matrix  $H$  is a normalized Hermitian complex Hadamard matrix.

Three conditions give structure of the diagonal matrices in  $\mathbf{D}$ .

- (D1)  $D^{[0]}$  has positive diagonal and for all  $c \in \mathbb{Z}_\omega$  we have  $D^{[-c]} = \overline{D^{[c]}}$ .
- (D2) There is an  $m \times m$  diagonal matrix  $\Delta^{[0]}$  with positive diagonal such that  $D^{[0]} = \Delta^{[0]} \otimes I_r$ .
- (D3) For each  $c \in \mathbb{Z}_\omega$  there is a diagonal matrix  $U^{[c]} \in (\{0\} \cup \mathbb{U})^{r \times r}$  and a diagonal matrix  $\Delta^{[c]}$  such that  $D^{[c]} = \Delta^{[c]} \otimes U^{[c]}$ . Further, if  $D^{[c]} = 0$  then  $U^{[c]} = 0$ .

These conditions will play a central role throughout the whole section. Once we make sure that they are satisfied, the problem  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  has all properties necessary to find a polynomial time equivalent **(H-STD)** problem. Then the following lemma provides us with the last part of the proof of Lemma 5.1.

**Lemma 5.3.** *Let  $C, \mathbf{D}$  satisfy conditions (C1), (C2) and (D1)–(D3). Let a matrix  $H$  and a family  $\mathbf{U} = (U^{[\mathbb{c}]})_{c \in \mathbb{Z}_\omega}$  be defined as in conditions (C1), (C2) and (D1)–(D3), respectively. Then*

$$\text{EVAL}^{\text{pin}}(C, \mathbf{D}) \equiv \text{EVAL}^{\text{pin}}(H, \mathbf{U}).$$

Before we give the proof of the Lemma, let us first develop a small technical result which will play an important role in that proof.

**Lemma 5.4.** *Let  $A \in \mathbb{C}^{m \times m}$  and  $A' \in \mathbb{C}^{m' \times m'}$  be  $\omega$ -algebraic. Let  $\mathbf{D} = (D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  be a family of  $m \times m$  diagonal matrices and  $\mathbf{D}' = (D'^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  a family of  $m' \times m'$  diagonal matrices. Let  $A'' = A \otimes A'$  and  $\mathbf{D}'' = (D^{\llbracket c \rrbracket} \otimes D'^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$ . There are projections  $\tau$  and  $\tau'$  such that for every digraph  $G$  and pinning  $\phi$  we have*

$$Z_{A'', \mathbf{D}''}(\phi, G) = Z_{A, \mathbf{D}}(\tau \circ \phi, G) \cdot Z_{A', \mathbf{D}'}(\tau' \circ \phi, G).$$

*Proof.* For convenience, we write the indices of  $A''$  as pairs according to the tensor product structure. That is

$$A''_{(i,k),(j,l)} = A_{ij} \cdot A'_{kl} \text{ for all } i, j \in [m] \text{ and } k, l \in [m'].$$

This holds analogously for the elements of  $\mathbf{D}''$ . We define  $\tau : [mm'] \rightarrow [m]$  and  $\tau' : [mm'] \rightarrow [m']$  by  $\tau(i, k) = i$  and  $\tau'(i, k) = k$  for all  $(i, k) \in [m] \times [m']$ .

Let  $G = (V, E)$  be a digraph and  $\phi$  a pinning w.r.t.  $A''$ . Define  $V' = V \setminus \text{def}(\phi)$ .

$$\begin{aligned} Z_{A'', \mathbf{D}''}(\phi, G) &= \sum_{\phi \subseteq \sigma : V \rightarrow [m] \times [m']} \prod_{uv \in E} A''_{\sigma(u), \sigma(v)} \prod_{v \in V'} (D^{\llbracket \partial(v) \rrbracket} \otimes D'^{\llbracket \partial(v) \rrbracket})_{\sigma(v), \sigma(v)} \\ &= \sum_{\phi \subseteq \sigma : V \rightarrow [m] \times [m']} \prod_{uv \in E} A_{\tau \circ \sigma(u), \tau \circ \sigma(v)} A'_{\tau' \circ \sigma(u), \tau' \circ \sigma(v)} \\ &\quad \cdot \prod_{v \in V'} D_{\tau \circ \sigma(v), \tau \circ \sigma(v)}^{\llbracket \partial(v) \rrbracket} \cdot D_{\tau' \circ \sigma(v), \tau' \circ \sigma(v)}^{\llbracket \partial(v) \rrbracket} \end{aligned}$$

For each configuration  $\sigma \supseteq \phi$  we can form two independent maps  $\sigma^*$  and  $\sigma'$  such that  $\tau \circ \phi \subseteq \sigma^* = \tau \circ \sigma$  and  $\tau' \circ \phi \subseteq \sigma' = \tau' \circ \sigma$ . Therefore we obtain

$$\begin{aligned} Z_{A'', \mathbf{D}''}(\phi, G) &= \left( \sum_{\tau \circ \phi \subseteq \sigma^* : V \rightarrow [m]} \prod_{uv \in E} A_{\sigma^*(u), \sigma^*(v)} \prod_{v \in V'} D_{\sigma^*(v), \sigma^*(v)}^{\llbracket \partial(v) \rrbracket} \right) \\ &\quad \cdot \left( \sum_{\tau' \circ \phi \subseteq \sigma' : V \rightarrow [m']} \prod_{uv \in E} A'_{\sigma'(u), \sigma'(v)} \prod_{v \in V'} D_{\sigma'(v), \sigma'(v)}^{\llbracket \partial(v) \rrbracket} \right) \end{aligned}$$

In other words,  $Z_{A'', \mathbf{D}''}(\phi, G) = Z_{A, \mathbf{D}}(\tau \circ \phi, G) \cdot Z_{A', \mathbf{D}'}(\tau' \circ \phi, G)$ .  $\square$

*Proof (of Lemma 5.3).* Define  $M = \varsigma \cdot vw^T$  and let  $\mathbf{\Delta} = (\Delta^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$  be a family of  $m \times m$  diagonal matrices defined as in conditions **(D2)** and **(D3)**. In particular,  $C = M \otimes H$  and for each  $c \in \mathbb{Z}_\omega$  we have  $D^{\llbracket c \rrbracket} = \Delta^{\llbracket c \rrbracket} \otimes U^{\llbracket c \rrbracket}$ . Then the following claim follows from Lemma 5.4.

*Claim 1.* There are mappings  $\tau$  and  $\tau'$  such that for every digraph  $G = (V, E)$  and every pinning  $\phi$ , we have

$$Z_{C, \mathbf{D}}(\phi, G) = Z_{M, \mathbf{\Delta}}(\tau \circ \phi, G) \cdot Z_{H, \mathbf{U}}(\tau' \circ \phi, G).$$

By Lemma 4.21 the function  $\text{EVAL}^{\text{pin}}(M, \mathbf{\Delta})$  is polynomial time computable and therefore Claim 1 implies the existence of a reduction witnessing  $\text{EVAL}^{\text{pin}}(C, \mathbf{D}) \leq \text{EVAL}^{\text{pin}}(H, \mathbf{U})$ .

It remains to prove the reducibility  $\text{EVAL}^{\text{pin}}(H, \mathbf{U}) \leq \text{EVAL}^{\text{pin}}(C, \mathbf{D})$ , the proof of which is slightly more complicated. The complications arise from the fact that there may be graphs

$G$  for which  $Z_{M,\Delta}(\tau \circ \phi, G) = 0$  implying  $Z_{C,D}(\phi, G) = 0$  although  $Z_{H,U}(\tau' \circ \phi, G)$  might be non-zero.

We will tackle this problem by  $(p \cdot \omega + 1)$ -thickening. Let  $G^{(p\omega+1)}$  be the graph obtained from  $G$  by this operation. Note that  $(p \cdot \omega + 1)\partial(v) \equiv \partial(v) \pmod{\omega}$  for all vertices  $v$  whence it thus follows by inspection that

$$Z_{H,U}(\tau' \circ \phi, G^{(p\omega+1)}) = Z_{H^{(p\omega+1)},U}(\tau' \circ \phi, G).$$

Since every entry of  $H$  is an  $\omega$ -th root of unity, we have  $H^{(p\omega+1)} = H$ . Therefore,

$$Z_{C,D}(\phi, G^{(p\omega+1)}) = Z_{M,\Delta}(\tau \circ \phi, G^{(p\omega+1)}) \cdot Z_{H,U}(\tau' \circ \phi, G).$$

We will show the following claim.

*Claim 2.* There is a computable  $p \in \mathbb{N}$  which depends only on  $M$  and  $\Delta$  such that  $Z_{H,U}(\tau' \circ \phi, G) \neq 0$  implies  $Z_{M,\Delta}(\tau \circ \phi, G^{(p\omega+1)}) \neq 0$ .

Before we give the proof let us see how this finishes the proof of the lemma. Given this  $p$  we can compute  $Z_{M,\Delta}(\tau \circ \phi, G^{(p\omega+1)})$  in polynomial time. If it is zero then we know that  $Z_{H,U}(\tau' \circ \phi, G)$  is and we are done. Otherwise, we can compute

$$\left( Z_{M,\Delta}(\tau \circ \phi, G^{(p\omega+1)}) \right)^{-1} \cdot Z_{C,D}(\phi, G^{(p\omega+1)}) = Z_{H,U}(\tau' \circ \phi, G).$$

This yields  $\text{EVAL}^{\text{pin}}(H, U) \leq \text{EVAL}^{\text{pin}}(C, D)$ .

**Proof of Claim 2.** Recall that  $Z_{M,\Delta}(\tau \circ \phi, G) = \varsigma^{|E|} \cdot Z_{vw^T, \Delta}(\tau \circ \phi, G)$ . We will therefore focus on  $Z_{vw^T, \Delta}(\tau \circ \phi, G)$ . Define  $V' = V \setminus \text{def}(\tau \circ \phi)$  and recall that by **(C1)** we have  $w = \lambda \cdot v$  for some positive  $\lambda$ . Therefore

$$\begin{aligned} Z_{vw^T, \Delta}(\tau \circ \phi, G) &= \sum_{\tau \circ \phi \subseteq \sigma: V \rightarrow [m]} \prod_{ab \in E} v_{\sigma(a)} w_{\sigma(b)} \prod_{a \in V'} \Delta_{\sigma(a)\sigma(a)}^{\llbracket \partial(a) \rrbracket} \\ &= \lambda^{|E|} \sum_{\tau \circ \phi \subseteq \sigma: V \rightarrow [m]} \prod_{a \in \text{def}(\phi)} v_{\sigma(a)}^{d(a)} \prod_{a \in V'} v_{\sigma(a)}^{d(a)} \Delta_{\sigma(a)\sigma(a)}^{\llbracket \partial(a) \rrbracket} \\ &= \lambda^{|E|} \prod_{a \in \text{def}(\phi)} v_{\tau \circ \phi(a)}^{d(a)} \sum_{\sigma: V' \rightarrow [m]} \prod_{a \in V'} v_{\sigma(a)}^{d(a)} \Delta_{\sigma(a)\sigma(a)}^{\llbracket \partial(a) \rrbracket} \end{aligned}$$

It thus follows that

$$\begin{aligned} Z_{vw^T, \Delta}(\tau \circ \phi, G^{(p\omega+1)}) &= \lambda^{|E|} \prod_{a \in \text{def}(\phi)} v_{\tau \circ \phi(a)}^{(p\omega+1) \cdot d_G(a)} \sum_{\sigma: V' \rightarrow [m]} \prod_{a \in V'} v_{\sigma(a)}^{(p\omega+1) \cdot d_G(a)} \Delta_{\sigma(a)\sigma(a)}^{\llbracket (p\omega+1) \cdot \partial_G(a) \rrbracket} \\ &= \lambda^{|E|} \prod_{a \in \text{def}(\phi)} v_{\tau \circ \phi(a)}^{(p\omega+1) \cdot d_G(a)} \prod_{a \in V'} \sum_{i=1}^m v_i^{(p\omega+1) \cdot d_G(a)} \Delta_{ii}^{\llbracket \partial_G(a) \rrbracket} \end{aligned}$$

By this calculation,  $Z_{vw^T, \Delta}(\tau \circ \phi, G^{(p\omega+1)})$  is non-zero for some  $p \in \mathbb{N}$ , if for each  $a \in V'$ ,

$$0 \neq \sum_{i=1}^m v_i^{(p\omega+1) \cdot d_G(a)} \Delta_{ii}^{\llbracket \partial_G(a) \rrbracket} \quad (33)$$

To finish the proof it suffices to prove, for each  $a \in V'$ , the existence of a  $p_a$  such that with  $p \geq p_a$  the inequality in (33) is satisfied. If further each  $p_a$  depends only on  $M$  and  $\Delta$ , then with  $p$  being the maximum of all these  $p_a$  the proof of the claim follows.

The assumption  $Z_{H,U}(\tau' \circ \phi, G) \neq 0$  implies that for each  $a \in V'$  the matrix  $U^{\llbracket \partial_G(a) \rrbracket} \neq 0$  and thus by condition (D3) the matrix  $D^{\llbracket \partial_G(a) \rrbracket}$  contains a non-zero diagonal entry. By the General Principles of Section 4.1 we may assume that  $G$  is connected. Further the reduction is trivial if  $G$  contains no edge, therefore we may assume further that  $d_G(a) \geq 1$  for all  $a \in V$ .

Fix an  $a \in V'$  and let  $i_a$  be the maximum index  $i \in [m]$  such that  $\Delta_{ii}^{\llbracket \partial_G(a) \rrbracket} \neq 0$ . If there is only one index  $i \in [m]$  such that  $\Delta_{ii}^{\llbracket \partial_G(a) \rrbracket} \neq 0$ , then the inequality in (33) holds for all  $p \geq p_a := 0$ . Otherwise, let  $z \in [m]$ , with  $z \neq i_a$  be maximal such that  $\Delta_{zz}^{\llbracket \partial_G(a) \rrbracket} \neq 0$ . The inequality (33) is satisfied if

$$\left| v_{i_a}^{(p\omega+1) \cdot d_G(a)} \Delta_{i_a i_a}^{\llbracket \partial_G(a) \rrbracket} \right| > \left| \sum_{i \neq i_a} v_i^{(p\omega+1) \cdot d_G(a)} \Delta_{ii}^{\llbracket \partial_G(a) \rrbracket} \right| \quad (34)$$

By the definition of  $z$  this is the case if

$$\left( \frac{v_{i_a}}{v_z} \right)^{(p\omega+1) \cdot d_G(a)} > \left| \sum_{i \neq i_a} \Delta_{ii}^{\llbracket \partial_G(a) \rrbracket} \right| \left| \Delta_{i_a i_a}^{\llbracket \partial_G(a) \rrbracket} \right|^{-1} \quad (35)$$

As  $d_G(a) \geq 1$ ,  $\omega \geq 1$  and  $0 < v_z < v_{i_a}$ , there is a  $p_a$  such that for all  $p \geq p_a$  the inequality (35) (and hence (33)) is satisfied. To finish the proof, observe that  $p_a$  depends only on  $\Delta$  and  $v_1, \dots, v_m$ .  $\square$

## 5.1 Satisfying Shape Conditions (C1) and (D1)

We will now show, in a sequence of several small steps, how to transform the initial problem  $\text{EVAL}^{\text{pin}}(A, D)$  into a problem satisfying the shape conditions. In each step, if transformation is not possible we will argue that this is due to the problem at hand being  $\#P$ -hard.

The first step will provide us with the transformation of  $\text{EVAL}^{\text{pin}}(A, D)$  into a problem satisfying (C1) and (D1).

**Lemma 5.5.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{n \times n}$  be a Hermitian  $\omega$ -algebraic matrix which is connected and non-bipartite and  $D \in \mathbb{R}_{\mathbb{A}}^{n \times n}$  a diagonal matrix of positive vertex weights. Then either  $\text{EVAL}^{\text{pin}}(A, D)$  is  $\#P$ -hard or the following holds.*

*There is a matrix  $C$  satisfying condition (C1) and a family  $\mathbf{D}$  of diagonal matrices which satisfies condition (D1) such that*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(C, \mathbf{D}).$$

*Further, there are two technical results following from the proof.*

$$(1) \ H(D^{\llbracket 0 \rrbracket; \mu}) \overline{H}^T = \text{tr}(D^{\llbracket 0 \rrbracket; \mu}) I_r \text{ for all } \mu \in [m].$$

$$(2) \ \text{There are constants } d_1, \dots, d_m \text{ such that } D^{\llbracket 0 \rrbracket; \mu} = d_\mu D^{\llbracket 0 \rrbracket; 1} \text{ for all } \mu \in [m].$$

We split the proof into two parts. The first of which is given in the following lemma.

**Lemma 5.6.** *Let  $A \in \mathbb{C}_{\mathbb{A}}^{n \times n}$  be a Hermitian  $\omega$ -algebraic matrix which is connected and non-bipartite and  $D \in \mathbb{R}_{\mathbb{A}}^{n \times n}$  a diagonal matrix of positive vertex weights. Either  $\text{EVAL}^{\text{pin}}(A, D)$  is  $\#P$ -hard or the following holds.*

*There is a Hermitian  $\omega$ -algebraic and twin-free matrix  $C$  and a family  $\mathbf{D} = (D^{[\mathbb{c}]})_{c \in \mathbb{Z}_{\omega}}$  of diagonal matrices which satisfies condition **(D1)** such that*

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(C, \mathbf{D}).$$

*The matrix  $C$  further has the following properties. There is a  $\varsigma \in \{-1, 1\}$  and positive vectors  $v, w \in \mathbb{R}_{\mathbb{A}}^m$  such that  $v_1 < \dots < v_m$  and  $w = \lambda v$  for some positive  $\lambda$  such that*

$$C = \begin{pmatrix} v_1 w_1 P^{11} & \dots & v_1 w_m P^{1m} \\ \vdots & \ddots & \vdots \\ v_m w_1 P^{m1} & \dots & v_m w_m P^{mm} \end{pmatrix}.$$

*For appropriate matrices  $P^{\mu\nu}$  of  $\omega$ -th roots of unity such that  $P_{*,1}^{\mu 1}$  and  $P_{1,*}^{1\mu}$  are constantly  $\varsigma$  for all  $\mu \in [m]$ .*

*Proof.* For convenience we will assume in the following that

$$|A_{ii}| \leq |A_{jj}| \text{ for all } i \leq j \in [n]. \quad (36)$$

This is possible w.l.o.g. by the Permutability Principle 4.3, since every matrix  $A$  satisfies this condition up to symmetric permutations of rows and columns. Let  $\mathbf{D}' = (D'^{[\mathbb{c}]})_{c \in \mathbb{Z}_{\omega}}$  with  $D'^{[\mathbb{c}]} = D$  for all  $c \in \mathbb{Z}_{\omega}$ . By Lemma 2.1 we have

$$Z_{A,D}(\phi, G) = Z_{A,\mathbf{D}'}(\phi, G) \quad \text{for all digraphs } G \text{ and all pinings } \phi \quad (37)$$

and therefore,  $\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(A, \mathbf{D}')$ . By Lemma 4.23 the problem  $\text{EVAL}^{\text{pin}}(A, \mathbf{D}')$  is  $\#P$ -hard, if  $\text{abs}(A)$  has rank at least 2. Assume therefore, that  $\text{abs}(A)$  has rank 1 that is,  $\text{abs}(A) = xy^T$  for non-negative real vectors  $x$  and  $y$ . The vectors  $x$  and  $y$  are positive. To see this, note that  $\text{abs}(A)$  is a block, because  $A$  is. On the other hand a value  $x_i = 0$  would contradict this fact, as then  $\text{abs}(A)_{i,*} = x_i y^T = 0$  implying the decomposability of  $\text{abs}(A)$ . Therefore for appropriate  $\omega$ -th roots of unity  $\zeta_{ij}$  we have

$$A_{ij} = x_i y_j \cdot \zeta_{ij} \text{ for all } i, j \in [n]. \quad (38)$$

By the Hermitianity of  $A$  we have  $\zeta_{11} \in \{-1, 1\}$ . Define  $\varsigma := \zeta_{11}$  and a diagonal  $n \times n$  matrix  $\Pi$  by  $\Pi_{ii} = \varsigma \cdot \overline{\zeta_{i1}}$  for all  $i \in [n]$ . Let  $A' = \Pi A \overline{\Pi}$ . The first column of this matrix satisfies  $A'_{i1} = \Pi_{ii} A_{i1} \overline{\Pi}_{11} = \varsigma \overline{\zeta_{i1}} \zeta_{i1} x_i y_1 \overline{\zeta_{11}} \zeta_{11} = \varsigma x_i y_1$  for all  $i \in [n]$ . As this follows similarly for the first row of  $A'$  we have

$$A'_{i1} = \varsigma |A'_{i1}| = \varsigma |A'_{1i}| = A'_{1i} \text{ for all } i \in [n]. \quad (39)$$

With  $\mathbf{D}'' = (D''^{[\mathbb{c}]})_{c \in \mathbb{Z}_{\omega}}$  defined by  $D''^{[\mathbb{c}]} = \Pi^c D'^{[\mathbb{c}]}$  the Root Of Unity Transfer Lemma 4.7 yields

$$Z_{A,\mathbf{D}'}(\phi, G) = f_{\Pi}(\phi) \cdot Z_{A',\mathbf{D}''}(\phi, G) \quad \text{for all digraphs } G \text{ and all pinings } \phi. \quad (40)$$



The function  $f_\Pi$  is polynomial time computable and non-zero for every  $\phi$ . By definition, all diagonal entries of  $\Pi$  are  $\omega$ -th roots of unity. Hence  $\Pi^{\omega^{-c}} = \overline{\Pi}^c$  for all  $c \in \mathbb{Z}_\omega$ , that is,  $\mathbf{D}''$  satisfies condition (D1).

We will now perform twin reduction. Let  $I_1, \dots, I_{n'}$  be the equivalence classes of the twin relation on  $A'$  and let  $\tau$  be the twin resolution mapping. By Lemma 4.5 we have

$$Z_{A', \mathbf{D}''}(\phi, G) = Z_{[A'], \mathbf{D}^{[A']}}(\tau \circ \phi, G) \text{ for all digraphs } G \text{ and all pinings } \phi. \quad (41)$$

Define  $C = [A']$  and  $\mathbf{D} = \mathbf{D}^{[A']} = (D^{[A'], \llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$ . The family  $\mathbf{D}$  therefore satisfies  $D_{ii}^{\llbracket c \rrbracket} = \sum_{\nu \in I_i} D_{\nu, \nu}^{\llbracket c \rrbracket}$  for all  $i \in [n']$  and all  $c \in \mathbb{Z}_\omega$ . It follows from the fact that  $\mathbf{D}''$  satisfies condition (D1) that this is also true for  $\mathbf{D}$ . Since  $C$  is the twin resolvent of  $A'$  we have

$$C_{ij} = A'_{\mu\nu} \text{ for some } \mu \in I_i, \nu \in I_j.$$

We may assume w.l.o.g. that  $1 \in I_1$  and that for all  $i, j \in [n']$  and all  $\mu \in I_i, \nu \in I_j$  we have  $|A'_{\mu\mu}| \leq |A'_{\nu\nu}|$  iff  $i \leq j$ . This is possible if we assume an appropriate ordering of the  $I_1, \dots, I_{n'}$ . We thus obtain, from equation (39),

$$C_{i1} = \varsigma |C_{i1}| = \varsigma |C_{1i}| = C_{1i} \text{ for all } i \in [n'] \quad (42)$$

and, as this was true for  $A$  and  $A'$ ,

$$|C_{ii}| \leq |C_{jj}| \text{ for all } i \leq j \in [n']. \quad (43)$$

With  $\text{rank abs}(A) = 1$  we have  $\text{rank abs}(C) = 1$  and still there are no zero entries in this matrix. There are thus positive vectors  $u$  and  $z$  such that  $\text{abs}(C) = uz^T$ . By the symmetry of  $\text{abs}(C)$  we have  $u_i z_j = u_j z_i$  for all  $i, j \in [n']$  which implies that  $u$  and  $z$  are linearly dependent with  $z_i = \frac{z_1}{u_1} \cdot u_i$ . Let  $\lambda = z_1 \cdot u_1^{-1}$ . This rephrases equation (43) to  $u_i^2 \lambda \leq u_j^2 \lambda$  for all  $i \leq j \in [n']$  and therefore the entries of  $u$  are ordered increasingly. Let  $v$  be the vector of increasingly ordered distinct entries of  $u$  and  $w$  the analogon for  $z$ . We have  $w = \lambda v$ . Let  $m$  be the length of  $w$ . The definition of  $C$  can thus be rephrased as

$$C = \begin{pmatrix} v_1 w_1 P^{11} & \dots & v_1 w_m P^{1m} \\ \vdots & \ddots & \vdots \\ v_m w_1 P^{m1} & \dots & v_m w_m P^{mm} \end{pmatrix}$$

for appropriate matrices  $P^{\mu\nu}$  of  $\omega$ -th roots of unity. From (42) it follows that  $P_{*,1}^{\mu 1}$  and  $P_{1,*}^{1\mu}$  are constant for all  $\mu \in [m]$  — each entry equals  $\varsigma$ . Combining equations (37), (40) and (41) yields,

$$Z_{A,D}(\phi, G) = f_\Pi(\phi) \cdot Z_{C,\mathbf{D}}(\tau \circ \phi, G) \text{ for all digraphs } G \text{ and all pinings } \phi.$$

This finishes the proof. □

*Proof (of Lemma 5.5).* Assume that  $\text{EVAL}^{\text{pin}}(A, D)$  is not  $\#P$ -hard. By Lemma 5.6 we have  $\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(C, \mathbf{D})$  for a family  $\mathbf{D}$  of diagonal matrices satisfying (D1) and

a matrix  $C$  which has the following properties. There are vectors  $v, w \in \mathbb{R}_{\mathbb{A}}^m$  satisfying  $0 < v_1 < \dots < v_m$  and  $w = \lambda v$  for some  $\lambda > 0$  such that

$$C = \begin{pmatrix} v_1 w_1 P^{11} & \dots & v_1 w_m P^{1m} \\ \vdots & \ddots & \vdots \\ v_m w_1 P^{m1} & \dots & v_m w_m P^{mm} \end{pmatrix}$$

for appropriate matrices  $P^{\mu\nu}$  of  $\omega$ -th roots of unity. By the Hermitianity of  $C$ , there are numbers  $m_1, \dots, m_m$  such that  $P^{\mu\nu}$  is an  $m_\mu \times m_\nu$  matrix and  $P^{\mu\nu} = \overline{P^{\nu\mu}}$  for all  $\mu, \nu \in [m]$ . We index  $C$  so as to explicate this structure. That is for  $\mu, \nu \in [m]$ ,  $i \in [m_\mu]$  and  $j \in [m_\nu]$  we let  $C_{(\mu,i)(\nu,j)} = v_\mu w_\nu P_{ij}^{\mu\nu}$ . Index the matrices  $D^{\llbracket c \rrbracket}$  analogously and write, for convenience,  $D_{ii}^{\llbracket c \rrbracket; \mu} := D_{(\mu,i)(\mu,i)}^{\llbracket c \rrbracket}$  for all  $i \in [m_\mu]$ .

*Claim 1.* For all  $\mu, \nu, \kappa \in [m]$  and  $i \in [m_\mu]$ ,  $j \in [m_\nu]$  we have  $\left| \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right| \leq \text{tr}(D^{\llbracket 0 \rrbracket; \kappa})$ . Furthermore, equality is assumed only if  $P_{j,*}^{\nu\kappa}$  and  $P_{i,*}^{\mu\kappa}$  are linearly dependent.

*Proof.* This is straightforward, we present the calculations for completeness. Application of the triangle inequality yields

$$\left| \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right| = \left| \sum_{k=1}^{m_\kappa} D_{k,k}^{\llbracket 0 \rrbracket; \kappa} \cdot \overline{P_{j,k}^{\nu\kappa}} \cdot P_{i,k}^{\mu\kappa} \right| \leq \sum_{k=1}^{m_\kappa} \left| D_{k,k}^{\llbracket 0 \rrbracket; \kappa} \cdot \overline{P_{j,k}^{\nu\kappa}} \cdot P_{i,k}^{\mu\kappa} \right| = \text{tr}(D^{\llbracket 0 \rrbracket; \kappa}).$$

Here, equality can be assumed only if all of the terms  $\overline{P_{j,k}^{\nu\kappa}} \cdot P_{i,k}^{\mu\kappa}$  are equal. ⊣

*Claim 2.*  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  is  $\#P$ -hard unless the following is true. For all  $i \in [m_\mu]$  and all  $j \in [m_\nu]$  we have either

$$\langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle = 0 \text{ for all } \kappa \in [m] \text{ or } \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle = \text{tr}(D^{\llbracket 0 \rrbracket; \kappa}) \text{ for all } \kappa \in [m]. \quad (44)$$

In particular the latter case occurs only if  $P_{i,*}^{\mu\kappa} = P_{j,*}^{\nu\kappa}$ .

*Proof.* Define, for every  $q \in \mathbb{N}$  the value  $p = q \cdot \omega + 1$  and a matrix  $C' = C'(p) = C^{(p)} D^{\llbracket 0 \rrbracket} C^{(p)}$ . For a given digraph  $G = (V, E)$ , let  $G_p$  be the result of 2-stretching followed by  $p$ -thickening. Note that  $p \cdot \partial(v) \equiv \partial(v) \pmod{\omega}$  for all  $v \in V$ . Thus we obtain for every pinning  $\phi$

$$Z_{C'(p), \mathbf{D}}(\phi, G) = Z_{C, \mathbf{D}}(\phi, G_p). \quad (45)$$

The matrix  $C'$  satisfies

$$\begin{aligned} C'_{(\mu,i)(\nu,j)} &= \sum_{\kappa=1}^m \sum_{k=1}^{m_\kappa} C_{(\mu,i)(\kappa,k)}^{(p)} \overline{C_{(\nu,j)(\kappa,k)}^{(p)}} D_{(\kappa,k)(\kappa,k)}^{\llbracket 0 \rrbracket} \\ &= v_\mu^p v_\nu^p \sum_{\kappa=1}^m \sum_{k=1}^{m_\kappa} w_\kappa^{2p} (P_{ik}^{\mu\kappa} \overline{P_{jk}^{\nu\kappa}})^p D_{k,k}^{\llbracket 0 \rrbracket; \kappa} \\ &= v_\mu^p v_\nu^p \sum_{\kappa=1}^m w_\kappa^{2p} \langle D^{\llbracket 0 \rrbracket; \kappa}, (P_{j,*}^{\nu\kappa})^{(p)} \bullet (P_{i,*}^{\mu\kappa})^{(p)} \rangle. \end{aligned}$$

The definition of  $p$  further implies  $(P_{ij}^{\mu\nu})^p = P_{ij}^{\mu\nu}$  for all  $i, j$  and all  $\mu, \nu$ . Hence

$$C'_{(\mu,i)(\nu,j)} = (v_\mu v_\nu)^{q\cdot\omega+1} \sum_{\kappa=1}^m w_\kappa^{2(q\cdot\omega+1)} \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \quad (46)$$

In particular all diagonal entries of  $C'$  are positive, as for all  $\mu \in [m]$ ,  $i \in [m_\mu]$  we have

$$C'_{(\mu,i)(\mu,i)} = v_\mu^{2(q\cdot\omega+1)} \sum_{\kappa=1}^m w_\kappa^{2(q\cdot\omega+1)} \text{tr}(D^{\llbracket 0 \rrbracket; \kappa}).$$

If there is a  $q$  such that the matrix  $\text{abs}(C')$  contains a block of rank at least 2, then by Lemma 4.23 the problem  $\text{EVAL}^{\text{pin}}(C', \mathbf{D})$  is  $\#P$ -hard. Then further, by equation (45),  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  will be  $\#P$ -hard. Assume therefore that, for all  $q$ , all blocks of  $\text{abs}(C')$  have rank 1. We shall show that under this assumption  $C$  satisfies (C1).

Consider some  $2 \times 2$  submatrix of  $\text{abs}(C')$  of the form

$$\begin{pmatrix} |C'_{(\mu,i)(\mu,i)}| & |C'_{(\mu,i)(\nu,j)}| \\ |C'_{(\nu,j)(\mu,i)}| & |C'_{(\nu,j)(\nu,j)}| \end{pmatrix}$$

By our assumption that for all  $q$  this submatrix is not a witness for the existence of a block of rank at least 2 in  $\text{abs}(C')$  we see that either its determinant is zero or  $C'_{(\mu,i)(\nu,j)} = 0$ . More precisely we arrive at the assumption that, for all  $\mu, \nu \in [m]$ ,  $i \in [m_\mu]$ ,  $j \in [m_\nu]$  and

$$\text{For all } q \in \mathbb{N} \text{ either } C'_{(\mu,i)(\nu,j)} = 0 \text{ or } |C'_{(\nu,j)(\nu,j)}| |C'_{(\mu,i)(\mu,i)}| = |C'_{(\mu,i)(\nu,j)}|^2. \quad (47)$$

If  $C'_{(\mu,i)(\nu,j)} = 0$  for infinitely many  $q$  then by the definition of  $C'$  in equation (46), we have

$$0 = \sum_{\kappa=1}^m (w_\kappa^{2\omega})^q w_\kappa^2 \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \quad \text{for all } q$$

which by Lemma 4.4 implies  $0 = \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle$  for all  $\kappa \in [m]$  — as claimed. Assume therefore that  $C'_{(\mu,i)(\nu,j)} = 0$  holds only for a finite number of  $q \in \mathbb{N}$ . Then clearly,  $|C'_{(\nu,j)(\nu,j)}| |C'_{(\mu,i)(\mu,i)}| = |C'_{(\mu,i)(\nu,j)}|^2$  must be true for infinitely many such  $q$ . By inspection of equation (46), this implies

$$\left| \sum_{\kappa=1}^m w_\kappa^{2(q\cdot\omega+1)} \text{tr}(D^{\llbracket 0 \rrbracket; \kappa}) \right|^2 = \left| \sum_{\kappa=1}^m w_\kappa^{2(q\cdot\omega+1)} \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right|^2$$

and thus

$$\sum_{\kappa=1}^m w_\kappa^{2p} \text{tr}(D^{\llbracket 0 \rrbracket; \kappa}) = \left| \sum_{\kappa=1}^m w_\kappa^{2p} \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right| \quad (48)$$

However, application of the triangle inequality yields

$$\left| \sum_{\kappa=1}^m w_\kappa^{2p} \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right| \leq \sum_{\kappa=1}^m w_\kappa^{2p} \left| \langle D^{\llbracket 0 \rrbracket; \kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right| \leq \sum_{\kappa=1}^m w_\kappa^{2p} \text{tr}(D^{\llbracket 0 \rrbracket; \kappa}).$$

By Claim 1 we have  $\left| \langle D^{[0];\kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right| \leq \text{tr}(D^{[0];\kappa})$  for each of the  $\kappa \in [m]$ . Equation (48) therefore implies the existence of some  $\alpha \in \mathbb{U}$  such that

$$0 = \sum_{\kappa=1}^m w_{\kappa}^{2p} \left( \text{tr}(D^{[0];\kappa}) - \alpha \langle D^{[0];\kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle \right).$$

As we may choose  $p$  arbitrarily large, depending only on  $D^{[0]}$  and  $C$ , Lemma 4.4 implies that

$$\alpha \langle D^{[0];\kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle = \text{tr}(D^{[0];\kappa}) \text{ for all } \kappa \in [m].$$

That is,  $P_{j,*}^{\nu\kappa} = \alpha P_{i,*}^{\mu\kappa}$  for all  $\kappa$ , in particular  $P_{j,1}^{\nu 1} = \alpha P_{i,1}^{\mu 1}$  which by our condition from Lemma 5.6 that  $P_{j,1}^{\nu 1} = P_{i,1}^{\mu 1}$  implies  $\alpha = 1$ .  $\dashv$

As  $C$  is twin-free, we see that, for every  $\mu \in [m]$  and all  $i \neq j \in [m_{\mu}]$  there is some  $\kappa \in [m]$  such that  $P_{j,*}^{\mu\kappa} \bullet P_{i,*}^{\mu\kappa}$  is not constant. Thus, by the above

$$\text{For all } \mu \in [m] \text{ and all } i \neq j \in [m_{\mu}] \text{ we have } \langle D^{[0];\kappa}, P_{j,*}^{\mu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle = 0 \text{ for all } \kappa \in [m]. \quad (49)$$

Fix some  $\kappa$  and define  $\Delta^{\kappa} := (D^{[0];\kappa})^{(1/2)}$ . Let  $T^{\mu\kappa} := P^{\mu\kappa} \Delta^{\kappa}$ , then

$$0 = \langle D^{[0];\kappa}, P_{j,*}^{\mu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle = \langle T_{i,*}^{\mu\kappa}, T_{j,*}^{\mu\kappa} \rangle \text{ for all } i \neq j \in [m_{\mu}].$$

That is,  $T^{\mu\kappa}$  has full row rank for all  $\mu, \kappa \in [m]$  and by the definition of  $T^{\mu\kappa}$  it has the same rank as  $P^{\mu\kappa}$ . Thus each  $P^{\mu\kappa}$  has full row rank and by  $P^{\mu\kappa} = \overline{P^{\kappa\mu}}$  it has full column rank, as well. Therefore each  $P^{\mu\nu}$  is non-singular. Let  $r = m_1$  be the rank of  $P^{11}$  therefore  $P^{1\kappa}$  being a non-singular  $r \times m_{\kappa}$  matrix for every  $\kappa \in [m]$  we see that  $m_1 = \dots = m_m = r$ . Altogether

$$\text{For all } \mu, \nu \in [m], P^{\mu\nu} \text{ is a non-singular } r \times r \text{ matrix.} \quad (50)$$

*Claim 3.* There are mappings  $\tau_1, \dots, \tau_m : [r] \rightarrow [r]$  such that for all  $\mu, \nu \in [m]$  we have

$$P_{ij}^{11} = P_{\tau_{\mu}(i), \tau_{\nu}(j)}^{\mu\nu} \text{ for all } i, j \in [r].$$

*Proof.* Consider the matrix

$$T^{*1} = \begin{pmatrix} T^{11} \\ \vdots \\ T^{m1} \end{pmatrix} = \begin{pmatrix} P^{11} \Delta^1 \\ \vdots \\ P^{m1} \Delta^1 \end{pmatrix}.$$

This matrix has rank  $r$  and by the above the first  $r$  rows of it form a set of independent vectors. In particular, for each  $\mu \in [m]$  and each  $j \in [r]$  there is an  $i \in [r]$  such that

$$\langle T_{i,*}^{11}, T_{j,*}^{\mu 1} \rangle \neq 0.$$

By  $\langle T_{i,*}^{11}, T_{j,*}^{\mu 1} \rangle = \langle D^{[0];1}, P_{j,*}^{\mu 1} \bullet P_{i,*}^{11} \rangle$  and Claim 2 we see that  $P_{j,*}^{\mu 1} = P_{i,*}^{11}$  and as  $C$  is twin-free we further see that for each  $\mu \in [m]$  this is unique. Thus define  $\tau_{\mu}(i) := j$  and by Hermitianity the claim follows.  $\dashv$

Define a permutation  $\pi : [m] \times [r] \rightarrow [m] \times [r]$  by  $\pi(\mu, i) := (\mu, \tau_\mu^{-1}(i))$ . By the above we have  $C_{(\mu,i)(\nu,j)} = v_\mu w_\nu P_{ij}^{\mu\nu} = v_\mu w_\nu P_{\tau_\mu(i)\tau_\nu(j)}^{11}$ . Thus the matrix  $C_{\pi\pi}$  satisfies

$$(C_{\pi\pi})_{(\mu,i)(\nu,j)} = C_{\pi(\mu,i)\pi(\nu,j)} = C_{\pi(\mu,\tau_\mu^{-1}(i))\pi(\nu,\tau_\nu^{-1}(j))} = v_\mu w_\nu P_{\tau_\mu(\tau_\mu^{-1}(i))\tau_\nu(\tau_\nu^{-1}(j))}^{11}$$

That is

$$(C_{\pi\pi})_{(\mu,i)(\nu,j)} = v_\mu w_\nu P_{ij}^{11}$$

Define  $H := \varsigma^{-1} \cdot P^{11}$ . We have  $C_{\pi\pi} = \varsigma \cdot vw^T \otimes H$  as desired.

It remains to prove the technical statements (1) and (2). To see (1), note that  $\langle D^{[0];\kappa}, P_{j,*}^{\nu\kappa} \bullet P_{i,*}^{\mu\kappa} \rangle$  translates to  $\langle D^{[0];\kappa}, H_{j,*} \bullet H_{i,*} \rangle = H(D^{[0];\kappa})\overline{H}^T$ . Statement (1) now follows by equation (49).

We shall show (2), that is, the linear dependence of the  $D^{[0];\mu}$ . Define the  $(r-1) \times r$  matrix  $H'$  by  $H'_{ij} = H_{ij}\overline{H}_{rj}$  for all  $j \in [r]$  and  $i \in [r-1]$  and let  $\text{diag}(D^{[0];\mu})$  be the vector of diagonal entries of  $D^{[0];\mu}$  then (1) implies that  $(HD^{[0];\mu}\overline{H}^T)_{rj} = 0$  for all  $j \neq r$  and all  $\mu \in [m]$ . This is equivalent to  $H'\text{diag}(D^{[0];\mu}) = 0$  for all  $\mu \in [m]$ . As  $H$  is non-singular we have  $\text{rank } H' = r-1$  and therefore all solutions to this system of linear equations are linearly dependent. This proves (2).  $\square$

## 5.2 The Remaining Conditions (C2), (D2) and (D3)

We now turn to the part of the proof devoted to the remaining conditions (C2), (D2) and (D3).

**Lemma 5.7.** *Let  $C, \mathbf{D}$  satisfy conditions (C1) and (D1) then either  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  is  $\#P$ -hard or conditions (C2) and (D2) hold.*

**Lemma 5.8.** *Let  $C, \mathbf{D}$  satisfy conditions (C1), (C2) and (D1) and (D2) then either  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  is  $\#P$ -hard or condition (D3) holds.*

The proofs of both lemmas are technically similar. Therefore we start by discussing the technical details they have in common. The most technical part is given by the Pre-Uniform Diagonal Lemma 5.9 below. Further, as the  $\#P$ -hardness proofs in both, Lemmas 5.7 and 5.8 are based on the same reduction, we discuss this reduction in Lemma 5.10.

**A Technical Tool.** We call a diagonal-matrix  $d \in \mathbb{C}^{m \times m}$  *pre-uniform* if there is a  $d \in \mathbb{C}$  such that for all  $i \in [m]$  we have  $D_{ii} \in \{0, d\}$ .

**Lemma 5.9 (Pre-Uniform Diagonal Lemma).** *Let  $H \in \mathbb{U}_\omega^{r \times r}$  be a non-singular matrix and  $D \in \mathbb{R}_\Delta^{r \times r}$  a non-negative diagonal matrix. Let  $K = \{k \in [r] \mid D_{kk} \neq 0\}$  be the set of non-zero diagonal entries in  $D$  then one of the following is true*

- *There is a computable  $p_0 \in \mathbb{N}$  such that for all  $p \geq p_0$  the matrix  $\text{abs}\left(HD^p\overline{H}^T\right)$  contains a block of rank at least 2.*
- *$D$  is pre-uniform and for all  $I \subseteq [r]$  the following holds. If  $H_{IK}$  is non-singular then it is a complex Hadamard matrix.*

*Proof.* The matrix  $B := HD^p\overline{H}^T$  satisfies, for all  $i, j \in [r]$ :

$$B_{ij} = \sum_{k=1}^r H_{ik}\overline{H}_{jk}D_{kk}^p = \sum_{k \in K} H_{ik}\overline{H}_{jk}D_{kk}^p = (H_{*,K}D_{KK}^p\overline{H}_{*,K}^T)_{ij}. \quad (51)$$

That is, for every  $I \subseteq [r]$  we have  $B_{II} = H_{IK}D_{KK}^p\overline{H}_{IK}^T$ . Let  $\kappa = |K|$  and fix a set  $I \subseteq [r]$  such that  $|I| = \kappa$  and  $H_{IK}$  has rank  $\kappa$ . Note that every principal  $2 \times 2$  submatrix of  $\text{abs}(B_{II})$  has non-zero determinant. To see this, fix an arbitrary such submatrix induced by distinct indices  $i, j \in [r]$ . Define a matrix  $X = H_{IK}D_{KK}^{(1/2)}$  which is non-singular since  $H_{IK}$  is. We have  $B = X\overline{X}^T$ . The determinant of the submatrix just defined is thus

$$\begin{vmatrix} |\langle X_{i,*}, X_{i,*} \rangle| & |\langle X_{i,*}, X_{j,*} \rangle| \\ |\langle X_{j,*}, X_{i,*} \rangle| & |\langle X_{j,*}, X_{j,*} \rangle| \end{vmatrix} = |\langle X_{i,*}, X_{i,*} \rangle| |\langle X_{j,*}, X_{j,*} \rangle| - |\langle X_{i,*}, X_{j,*} \rangle|^2$$

Using the Cauchy-Schwarz inequality, the non-singularity of  $X$  implies that the above determinant is non-zero since

$$|\langle X_{i,*}, X_{j,*} \rangle|^2 < |\langle X_{i,*}, X_{i,*} \rangle| |\langle X_{j,*}, X_{j,*} \rangle|.$$

Therefore, every principal  $2 \times 2$  submatrix of  $\text{abs}(B_{II})$  has non-zero determinant. The existence of a block of rank at least two in  $\text{abs}(B_{II})$  is thus guaranteed, if we find a non-zero off-diagonal entry. Hence, to finish the proof it remains to show the following: If there is no computable  $p_0$  such that for all  $p \geq p_0$  the matrix  $B_{II}$  contains a non-zero off-diagonal entry, then  $D$  is pre-uniform and  $H_{IK}$  complex Hadamard.

For every pair of values  $i, j \in I$  define a family  $\mathcal{Z}_{ij}$  of equivalence classes  $Z \in \mathcal{Z}_{ij}$  such that  $k, k' \in Z$  if, and only if  $H_{ik}\overline{H}_{jk} = H_{ik'}\overline{H}_{jk'}$ . Define for each such  $Z \in \mathcal{Z}_{ij}$  the value  $\zeta_Z := H_{ik}\overline{H}_{jk}$  for some  $k \in Z$ . Furthermore, define a family  $\mathcal{J}$  of equivalence classes induced by the equality of diagonal entries of  $D_{KK}$ . That is, for each  $J \in \mathcal{J}$  we have  $j, j' \in J$  iff  $D_{jj} = D_{j'j'}$  and denote by  $d_J$  the corresponding diagonal value of  $D$ . We obtain, for all  $i, j \in I$

$$B_{ij} = \sum_{k \in K} H_{ik}\overline{H}_{jk}D_{kk}^p = \sum_{J \in \mathcal{J}} d_J^p \sum_{Z \in \mathcal{Z}_{ij}} \zeta_Z |J \cap Z|$$

By Lemma 4.4 there is some  $p_0$  such that the following holds. For all  $p \geq p_0$  if  $B_{ij}$  is zero then, for every  $J \in \mathcal{J}$ ,

$$0 = \sum_{Z \in \mathcal{Z}_{ij}} \zeta_Z |J \cap Z| = \sum_{k \in J} H_{ik}\overline{H}_{jk}$$

As this is true for all  $i \neq j \in I$  the matrix  $H_{IJ}$  is non-singular and complex Hadamard. This implies that  $J = K$ , that is,  $D$  is pre-uniform.  $\square$

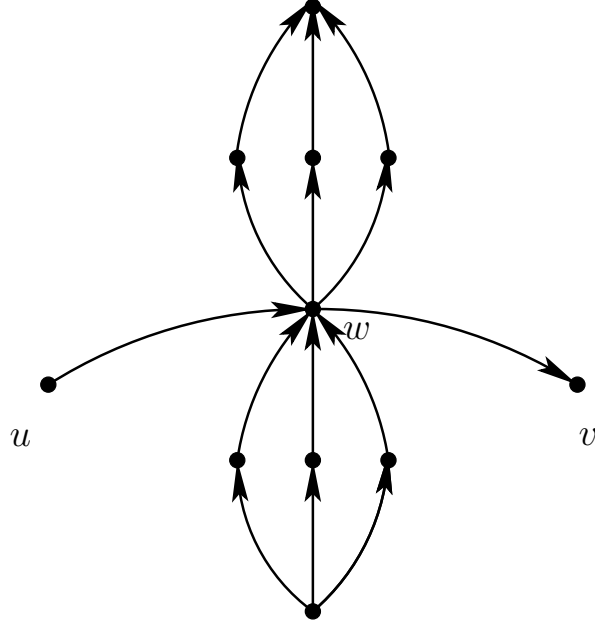
### The #P-hardness construction.

**Lemma 5.10.** *Let  $C \in \mathbb{C}_{\mathbb{A}}^{m \times m}$  and  $\mathbf{D}$  a family of diagonal matrices which satisfy (C1) and (D1). For all  $p, q \in \mathbb{N}$ , there is a diagonal matrix*

$$\Theta = \Theta(p, q) = \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} D^{[0];\mu} \left| \sum_{\kappa=1}^m v_{\kappa}^p D^{[p];\kappa} \right|^{2q} \quad (52)$$

such that the following is true.

*If  $\text{abs}(H\Theta\overline{H}^T)$  contains a block of rank at least 2 then  $\text{EVAL}^{pin}(C, \mathbf{D})$  is #P-hard.*

Figure 1: The reduction template  $T_{p,q}$  for  $p = 3, q = 1$ .

*Proof.* We define a *reduction template*  $T_{p,q}$  which will be used in the following reductions. This template is a digraph  $T_{p,q} = (V_{p,q}, E_{p,q})$  with two terminal vertices  $u$  and  $v$  which are connected by a length 2 path with middle vertex  $w$ . The most important subgraph of this template is a graph  $P(p)$ , which consists of two vertices  $b$  and  $a$  connected by  $p$  many paths of length 2 directed from  $b$  to  $a$ . Then,  $q$  many disjoint copies of  $P(p)$  are attached to  $w$  by identifying their terminal vertex  $a$  with  $w$  and further  $q$  copies of  $P(p)$  are attached by identifying their terminal vertex  $b$  with  $w$ . Figure 1 illustrates the construction. Its formal definition is given by

$$\begin{aligned} V_{p,q} &= \{u, v, w, x_i, x_{ij}, y_{ij}, y_i \mid i \in [q], j \in [p]\} \\ E_{p,q} &= \{uw, vw, x_i x_{ij}, x_{ij} w, w y_{ij}, y_{ij} y_i \mid i \in [q], j \in [p]\} \end{aligned}$$

For a given digraph  $G$ , let  $G'$  be the graph obtained from  $G$  by replacing every edge  $uv$  by a distinct copy of  $T_{p,q}$ . Let  $\phi$  be a pinning of  $G$ , then

$$Z_{C', \mathbf{D}}(\phi, G) = Z_{C, \mathbf{D}}(\phi, G') \quad (53)$$

where  $C'$  is a matrix whose structure we will analyze in the following. We start the analysis by observing a technical detail. We have, by Lemma 5.5(1),

$$CD^{\llbracket 0 \rrbracket} C = (vv^T) \otimes \sum_{\nu=1}^m w_\nu^2 H D^{\llbracket 0 \rrbracket; \nu} \overline{H}^T = (vv^T) \otimes \sum_{\nu=1}^m w_\nu^2 \text{tr}(D^{\llbracket 0 \rrbracket; \nu}) I_r$$

Condition (D1) implies that  $\text{tr}(D^{\llbracket 0 \rrbracket; \nu})$  is positive for all  $\nu$  and thus there is some positive  $\gamma$  such that

$$CD^{\llbracket 0 \rrbracket} C = (vv^T) \otimes \gamma I_r. \quad (54)$$

Here  $I_r$  denotes the  $r \times r$  identity matrix. Denote by  $Z_{C, \mathbf{D}}(i, j; T_{p,q})$  the partition function of  $T_{p,q}$  with vertex  $u$  pinned to  $i$  and  $v$  pinned to  $j$ . We have  $C'_{ij} = Z_{C, \mathbf{D}}(i, j; T_{p,q})$  for all  $i, j$ . Further the definition of  $T_{p,q}$  directly implies that  $C' = C\Delta C$  for some diagonal matrix  $\Delta = \Delta(p, q)$ . In the following we will index  $\Delta$  by pairs  $(\mu, i) \in [m] \times [r]$  and further define  $\Delta_{ii}^\mu = \Delta_{(\mu, i)(\mu, i)}$ . We obtain

$$\Delta_{i,i}^\mu = D_{i,i}^{[0];\mu} \left( \sum_{\kappa=1}^m \sum_{k=1}^r D_{k,k}^{[p];\kappa} \left( CD^{[0]}C \right)_{(\mu,i),(\kappa,k)}^p \right)^q \left( \sum_{\kappa=1}^m \sum_{k=1}^r D_{k,k}^{[-p];\kappa} \left( CD^{[0]}C \right)_{(\kappa,k),(\mu,i)}^p \right)^q$$

Applying equation (54) we see that, for all  $(\kappa, k), (\mu, i) \in [m] \times [r]$ ,

$$\left( CD^{[0]}C \right)_{(\mu,i),(\kappa,k)}^p = \left( CD^{[0]}C \right)_{(\kappa,k),(\mu,i)}^p = v_\kappa^p v_\mu^p \cdot \gamma^p \cdot (I_r)_{k,i}$$

which is zero unless  $k = i$ . By condition **(D1)** we have  $D^{[-p]} = \overline{D^{[p]}}$  and thus we can rewrite

$$\begin{aligned} \Delta_{i,i}^\mu &= D_{i,i}^{[0];\mu} \left( \sum_{\kappa=1}^m D_{i,i}^{[p];\kappa} v_\kappa^p v_\mu^p \cdot \gamma^p \right)^q \left( \sum_{\kappa=1}^m \overline{D_{i,i}^{[p];\kappa}} v_\kappa^p v_\mu^p \cdot \gamma^p \right)^q \\ &= v_\mu^{2pq} \gamma^{2pq} D_{i,i}^{[0];\mu} \left( \sum_{\kappa=1}^m v_\kappa^p D_{i,i}^{[p];\kappa} \right)^q \overline{\left( \sum_{\kappa=1}^m v_\kappa^p D_{i,i}^{[p];\kappa} \right)^q} \end{aligned}$$

And thus

$$\Delta_{i,i}^\mu = v_\mu^{2pq} \gamma^{2pq} D_{i,i}^{[0];\mu} \left| \sum_{\kappa=1}^m v_\kappa^p D_{i,i}^{[p];\kappa} \right|^{2q} \quad (55)$$

A direct computation yields

$$C\Delta C = vv^T \otimes H \left( \sum_{\mu=1}^m w_\mu^2 \Delta^\mu \right) \overline{H}^T. \quad (56)$$

and by equation (55) we obtain

$$\sum_{\mu=1}^m w_\mu^2 \Delta^\mu = \gamma^{2pq} \sum_{\mu=1}^m w_\mu^2 v_\mu^{2pq} D^{[0];\mu} \left| \sum_{\kappa=1}^m v_\kappa^p D_{i,i}^{[p];\kappa} \right|^{2q} = \gamma^{2pq} \cdot \Theta$$

where the last equality follows from the definition of  $\Theta = \Theta(p, q)$  in equation (52). Equation (56) then rephrases to

$$C\Delta C = vv^T \otimes H (\gamma^{2pq} \Theta) \overline{H}^T = \gamma^{2pq} \cdot vv^T \otimes H \Theta \overline{H}^T.$$

It thus follows that  $\text{abs}(C\Delta C)$  has a block of rank at least 2 iff  $\text{abs}(H\Theta\overline{H}^T)$  does. Assume that  $\text{abs}(H\Theta\overline{H}^T)$  contains a block of rank at least 2. Then  $\text{EVAL}^{\text{pin}}(C', \mathbf{D})$  is  $\#P$ -hard by Lemma 4.23. Equation (53) implies that  $\text{EVAL}^{\text{pin}}(C', \mathbf{D}) \leq \text{EVAL}^{\text{pin}}(C, \mathbf{D})$ . This finishes the proof.  $\square$



**The proofs of Lemma 5.7 and 5.8.**

*Proof (of Lemma 5.7).* Assume that  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  is not  $\#P$ -hard, we shall show that **(C2)** and **(D2)** are satisfied. Fix a positive  $p$  such that  $\llbracket p \rrbracket = 0$ . Let  $\Theta = \Theta(p, q)$  the matrix defined in equation (52). By Lemma 5.10, for all  $p, q \in \mathbb{N}$  the matrix  $\text{abs}\left(H\Theta\overline{H}^T\right)$  contains no blocks of rank at least 2. Recall the definition of  $\Theta = \Theta(p, q)$  and note that our choice of  $p$  yields,

$$\Theta = \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} D^{\llbracket 0 \rrbracket; \mu} \left| \sum_{\kappa=1}^m v_{\kappa}^p D^{\llbracket p \rrbracket; \kappa} \right|^{2q} = \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} D^{\llbracket 0 \rrbracket; \mu} \left( \sum_{\kappa=1}^m v_{\kappa}^p D^{\llbracket 0 \rrbracket; \kappa} \right)^{2q}$$

The second equality follows by condition **(D1)** as the absolute values  $|\cdot|$  are inessential for  $D^{\llbracket 0 \rrbracket}$ . By Lemma 5.5(2), we have

$$\Theta = \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} d_{\mu} D^{\llbracket 0 \rrbracket; 1} \left( \sum_{\kappa=1}^m v_{\kappa}^p d_{\kappa} D^{\llbracket 0 \rrbracket; 1} \right)^{2q}.$$

Define  $f(p, q) := \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} d_{\mu} (\sum_{\kappa=1}^m v_{\kappa}^p d_{\kappa})^{2q}$  which is positive for all  $p, q \in \mathbb{N}$ . Then

$$\Theta = \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} d_{\mu} \left( \sum_{\kappa=1}^m v_{\kappa}^p d_{\kappa} \right)^{2q} (D^{\llbracket 0 \rrbracket; 1})^{2q+1} = f(p, q) (D^{\llbracket 0 \rrbracket; 1})^{2q+1}.$$

For notational convenience let  $D := D^{\llbracket 0 \rrbracket; 1}$ . Then

$$H\Theta H^T = H(f(p, q) \cdot D^{2q+1}) \overline{H}^T = f(p, q) H D^{2q+1} \overline{H}^T$$

which implies that  $\text{abs}\left(H\Theta\overline{H}^T\right)$  contains a block of rank at least 2 iff  $\text{abs}\left(H D^{2q+1} \overline{H}^T\right)$  does.

We therefore arrive at the assumption that for all  $q \in \mathbb{N}$  the matrix  $\text{abs}\left(H D^{2q+1} \overline{H}^T\right)$  does not contain a block of row rank at least 2. The Pre-Uniform Diagonal Lemma 5.9 thus implies that  $H$  is complex Hadamard and  $D = \alpha I_r$  for some  $\alpha$ . This proves **(C2)**. Let  $\Delta_{\mu\mu}^{\llbracket 0 \rrbracket} = d_{\mu} \alpha$  with the  $d_{\mu}$  as given by Lemma 5.5(2). Then  $D^{\llbracket 0 \rrbracket} = \Delta^{\llbracket 0 \rrbracket} \otimes I_r$  which proves **(D2)**.  $\square$

*Proof (of Lemma 5.8).* Assume that  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  is not  $\#P$ -hard, we shall show that **(D3)** is satisfied for  $D^{\llbracket c \rrbracket}$  for all  $c \in \mathbb{Z}_{\omega}$ . Fix an arbitrary  $c \in \mathbb{Z}_{\omega}$  and let  $\Gamma_c = \{p \in \mathbb{N} \mid p \equiv c \pmod{\omega}\}$  be the set of natural numbers which are congruent to  $c$  modulo  $\omega$ . That is, we have  $\llbracket p \rrbracket = c$  for all  $p \in \Gamma_c$ . Let  $\Theta = \Theta(p, q)$  be the matrix defined in equation (52). By Lemma 5.10 we have

For all  $p, q \in \mathbb{N}$  the matrix  $\text{abs}\left(H\Theta\overline{H}^T\right)$  contains no blocks of rank at least 2.

We shall see how this implies condition **(D3)** for  $c$ . Assume from now on that  $p \in \Gamma_c$ . Then by the definition of  $\Theta = \Theta(p, q)$  in equation (52) we have

$$\begin{aligned} \Theta &= \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} D^{\llbracket 0 \rrbracket; \mu} \left| \sum_{\kappa=1}^m v_{\kappa}^p D^{\llbracket p \rrbracket; \kappa} \right|^{2q} \\ &= \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^{2pq} \Delta_{\mu\mu}^{\llbracket 0 \rrbracket} \left| \sum_{\kappa=1}^m v_{\kappa}^p D^{\llbracket c \rrbracket; \kappa} \right|^{2q} \end{aligned}$$

where the last equality follows from  $\llbracket p \rrbracket = c = \llbracket c \rrbracket$  and our assumption that condition **(D2)** is satisfied. Let  $f(x) := \left( \sum_{\mu=1}^m w_{\mu}^2 v_{\mu}^x \Delta_{\mu\mu}^{\llbracket 0 \rrbracket} \right)$  and define

$$\Delta = \left| \sum_{\kappa=1}^m v_{\kappa}^p D_{\kappa}^{\llbracket c \rrbracket; \kappa} \right| \quad (57)$$

Then  $\Theta = f(2pq) \cdot \Delta^{2q}$  and we have  $H\Theta\overline{H}^T = H(f(2pq) \cdot \Delta^{2q})\overline{H}^T = f(2pq)H\Delta^{2q}\overline{H}^T$ . That is, the existence of a block of rank 2 in  $\text{abs}\left(H\Theta\overline{H}^T\right)$  is equivalent to the existence of such a block in  $\text{abs}\left(H\Delta^{2q}\overline{H}^T\right)$  and thus it follows from our assumption that

$$\text{For all } p, q \in \mathbb{N} \text{ the matrix } \text{abs}\left(H\Delta^{2q}\overline{H}^T\right) \text{ does not contain a block of rank at least 2.} \quad (58)$$

*Claim 1.* For all  $p \in \Gamma_c$  the matrix  $\Delta = \Delta(p)$  is pre-uniform.

*Proof.* Assume otherwise. That is, fix a  $p \in \Gamma_c$  such that  $\Delta(p)$  is not pre-uniform. Then the Pre-Uniform Diagonal Lemma 5.9 implies that there is a  $q$  such that  $\text{abs}\left(H\Delta^{2q}\overline{H}^T\right)$  contains a block of rank at least 2, in contradiction to equation (58).  $\dashv$

In the above claim, we used the parameter  $q$  to show that  $\Delta$  is pre-uniform irrespective of our choice of  $p \in \Gamma_c$ . In the following we will show that choosing  $p$  large enough we can infer condition **(D3)** for  $c$ . To achieve this, we will prove the following two statements

*Claim 2.* There is a  $p_0$  such that for all  $p \in \Gamma_c$  with  $p \geq p_0$ ,

$$\text{If } \Delta_{ii} = \Delta(p)_{ii} = 0 \text{ then for all } \mu \in [m] \text{ we have } D_{ii}^{\llbracket c \rrbracket; \mu} = 0.$$

*Proof.* Fix an  $i \in [r]$ . By the definition of  $\Delta$  in equation (57) we see that  $\Delta_{ii} = 0$  if, and only if,

$$0 = \sum_{\kappa=1}^m v_{\kappa}^p D_{ii}^{\llbracket c \rrbracket; \kappa}.$$

If this equation is satisfied for all  $p$ , Lemma 4.4 implies the existence of values  $p_i$  such that for all  $p \in \Gamma_c$  with  $p \geq p_i$  we have  $D_{ii}^{\llbracket c \rrbracket; \mu} = 0$  for all  $\mu \in [m]$ . We derive such a  $p_i$  for each  $i \in [r]$  and the claim follows for  $p_0 = \max\{p_1, \dots, p_r\}$ .  $\dashv$

*Claim 3.* There is a  $p_{=}$  in  $\mathbb{N}$  such that for all  $p \in \Gamma_c$  with  $p \geq p_{=}$  and all  $i, j \in [r]$  we have that

$$\Delta_{ii} = \Delta_{jj} \text{ implies that there is a } \zeta_{ij} \in \mathbb{U} \text{ such that } D_{ii}^{\llbracket c \rrbracket; \mu} = \zeta_{ij} D_{jj}^{\llbracket c \rrbracket; \mu} \text{ for all } \mu \in [m].$$

*Proof.* By the definition of  $\Delta$  the assumption  $\Delta_{ii} = \Delta_{jj}$  is equivalent to

$$\left| \sum_{\kappa=1}^m v_{\kappa}^p D_{ii}^{\llbracket c \rrbracket; \kappa} \right| = \left| \sum_{\kappa=1}^m v_{\kappa}^p D_{jj}^{\llbracket c \rrbracket; \kappa} \right|$$

Or likewise, there is a  $\zeta_{ij} \in \mathbb{U}$  such that

$$0 = \sum_{\kappa=1}^m v_{\kappa}^p \left( D_{ii}^{[\mathbb{c}];\kappa} - \zeta_{ij} D_{jj}^{[\mathbb{c}];\kappa} \right).$$

By Lemma 4.4 there is a  $p_{ij}$  such that for all  $p \geq p_{ij}$ , the above implies that all coefficients  $D_{ii}^{[\mathbb{c}];\kappa} - \zeta_{ij} D_{jj}^{[\mathbb{c}];\kappa}$  are zero. The claim follows with  $p_{=} = \max\{p_{ij} \mid i \neq j \in [r]\}$ .  $\dashv$

With these three claims we are now able to finish the proof of the lemma. Let  $p \in \Gamma_c$  such that  $p \geq \max\{p_0, p_{=}\}$  with  $p_0$  and  $p_{=}$  as in Claims 2 and 3. We will argue by considering the diagonal entries of  $\Delta = \Delta(p)$ . Define  $M = \{\mu \in [m] \mid D^{[\mathbb{c}];\mu} \neq 0\}$  and let  $\Lambda = \{i \in [r] \mid \Delta_{ii} \neq 0\}$ .

If  $\Lambda = \emptyset$  then Claim 2 implies that  $D^{[\mathbb{c}]} = 0$  and the proof follows with  $\Delta^{[\mathbb{c}]} = 0$  and  $U^{[\mathbb{c}]} = 0$ .

Assume therefore that  $\Lambda \neq \emptyset$  and fix some  $a \in \Lambda$ . As  $\Delta$  is pre-uniform by Claim 1 we have  $\Delta_{ii} = \Delta_{aa}$  for all  $i \in \Lambda$ . By Claim 3 this implies that

$$D_{ii}^{[\mathbb{c}];\mu} = \zeta_{ia} D_{aa}^{[\mathbb{c}];\mu} \text{ for all } \mu \in M, i \in \Lambda.$$

Define  $\Delta_{\mu\mu}^{[\mathbb{c}]} = D_{aa}^{[\mathbb{c}];\mu}$  for every  $\mu$  and note that  $D_{aa}^{[\mathbb{c}];\mu} = 0$  if, and only if  $\mu \notin M$ . Define  $U_{ii}^{[\mathbb{c}]} = \zeta_{ia}$  for all  $i \in [r]$ . Then  $D^{[\mathbb{c}]} = \Delta^{[\mathbb{c}]} \otimes U^{[\mathbb{c}]}$ .  $\square$

### 5.3 Finishing the Proof of Lemma 5.1

Let  $A$  be a connected non-bipartite  $\omega$ -algebraic Hermitian matrix and  $D$  a diagonal matrix of positive vertex weights. By Lemma 5.5 either  $\text{EVAL}^{\text{pin}}(A, D)$  is  $\#P$ -hard or the following holds. There is a matrix  $C$  satisfying condition **(C1)** and a family  $\mathbf{D}$  of diagonal matrices which satisfies condition **(D1)** such that,

$$\text{EVAL}^{\text{pin}}(A, D) \equiv \text{EVAL}^{\text{pin}}(C, \mathbf{D}).$$

Further, by Lemmas 5.7 and 5.8 the problem  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  either is  $\#P$ -hard or the matrix  $C$  satisfies conditions **(C1)**–**(C2)** and the family  $\mathbf{D}$  satisfies **(D1)**–**(D3)**. By Lemma 5.3 we then have

$$\text{EVAL}^{\text{pin}}(C, \mathbf{D}) \equiv \text{EVAL}^{\text{pin}}(H, \mathbf{U})$$

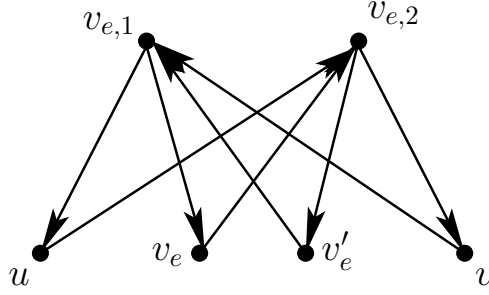
where  $H$  and  $\mathbf{U}$  define an **(H-STD)** problem. This finishes the proof.

## 6 Hadamard Components

In this section we will prove Theorem 3.5 by proving the following two lemmas.

**Lemma 6.1.** *Let  $H$  be an  $\omega$ -algebraic  $n \times n$  matrix and  $\mathbf{D}$  a family of diagonal matrices defining an **(H-STD)**-problem. Then either  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is  $\#P$ -hard or  $H$  and  $\mathbf{D}$  satisfy conditions **(GC)**, **(R1)** through **(R5)** and the Affinity Condition **(AF)**.*

**Lemma 6.2.** *Let  $A$  be  $\omega$ -algebraic with underlying  $n \times n$  block  $H$  and  $\mathbf{D}$  a family of diagonal matrices defining a **(B-H-STD)**-problem. Then either  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is  $\#P$ -hard or  $H$  and  $\mathbf{D}$  satisfy conditions **(GC)**, **(B-R1)** through **(B-R5)** and the Affinity Condition **(B-AF)**.*

Figure 2: The gadget for  $q = 1$ 

*Proof (of Theorem 3.5).* Let  $A$  be an  $\omega$ -algebraic matrix and  $\mathbf{D}$  a family of diagonal matrices defining either an **(H-STD)** problem or a **(B-H-STD)** problem.

If  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is not  $\#P$ -hard then the following holds. If  $A$  and  $\mathbf{D}$  define an **(H-STD)** problem then Lemma 6.1 implies that  $A$  and  $\mathbf{D}$  satisfy conditions **(GC)**, **(R1)** through **(R5)** and the Affinity Condition **(AF)**. If  $A$  and  $\mathbf{D}$  define a **(B-H-STD)** problem then Lemma 6.2 implies that  $A$  and  $\mathbf{D}$  satisfy conditions **(GC)**, **(B-R1)** through **(B-R5)** and the Affinity Condition **(B-AF)**. This finishes the proof of the Theorem.  $\square$

Throughout the section,  $n$  and  $\omega$  will have a fixed meaning. That is  $H$  will be an  $\omega$ -algebraic  $n \times n$  matrix. We will discuss the non-bipartite case in order to prove Lemma 6.1. In a sequence of several steps the proof will show that the problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is  $\#P$ -hard unless the conditions **(GC)**, **(R1)** through **(R5)** and the Affinity Condition **(AF)** are satisfied. This will be done in an inductive manner always relying on the conditions for which we have shown this so far. The proof of Lemma 6.2 follows by similar means, therefore we omit it. The interested reader may find the proof in [Thu09].

### 6.1 The Group Condition (GC)

The first step of the proof is to enable a group theoretic description of the matrix  $H$  underlying the **(H-STD)** problem at hand.

**Lemma 6.3.** *Let  $H$  be a matrix and  $\mathbf{D}$  a family of diagonal matrices defining an **(H-STD)**-problem. If  $H$  does not satisfy the group condition **(GC)** then  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is  $\#P$ -hard.*

*Proof.* Let  $G = (V, E)$  be a given digraph and  $\phi$  a pinning. Let  $G_q = (V_q, E_q)$  be the digraph obtained from  $G$  by

$$\begin{aligned} V_q &:= V \cup \{v_e, v'_e, v_{e,1}, \dots, v_{e,2q} \mid e \in E\} \\ E_q &:= \{uv_{e,2i}, v_{e,2i-1}u, v_{e,2i}v, vv_{e,2i-1} \mid i \in [q], e = uv \in E\} \\ &\quad \cup \{v_e v_{e,2i}, v_{e,2i-1}v_e, v_{e,2i}v'_e, v'_e v_{e,2i-1} \mid i \in [q], e \in E\} \end{aligned}$$

We can think of  $G_q$  being obtained from  $G$  by replacing every edge by a distinct copy of a graph  $\Gamma_q$  which, for  $q = 1$  is illustrated in Figure 2. Let  $i, j, a, b$  be spins assigned to  $u, v, v_e, v'_e$ .

This witnesses a reduction  $\text{EVAL}^{\text{pin}}(C^{[q]}) \leq \text{EVAL}^{\text{pin}}(H, \mathbf{D})$  with

$$\begin{aligned} C_{ij}^{[q]} &= \sum_{a=1}^n \sum_{b=1}^n \left( \sum_{c=1}^n H_{ic} H_{cj} H_{ac} H_{cb} \right)^q \left( \sum_{c=1}^n H_{ci} H_{jc} H_{ca} H_{bc} \right)^q \\ &= \sum_{a=1}^n \sum_{b=1}^n |\langle H_{a,*} \bullet H_{b,*}, H_{j,*} \bullet H_{i,*} \rangle|^{2q} \end{aligned}$$

By an argument based on  $C_{ij}^{[q]}$  for  $i, j \in [n]$  we will see in the following that  $\text{EVAL}^{\text{pin}}(C^{[q]})$  is #P-hard if  $H$  does not satisfy the group condition. We will not give a direct proof, but we will rather show that,

if there are  $a', b' \in [n]$  such that  $H_{a',*} \bullet H_{b',*} \notin R(H)$  then  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is #P-hard.

To see that this finishes our proof, we shall prove that

*Claim 1.* If  $H_{i,*} \bullet H_{j,*} \in R(H)$  for all  $i, j \in [n]$  then  $H$  satisfies (GC).

*Proof.* If  $H_{i,*} \bullet H_{j,*} \in R(H)$  for all  $i, j \in [n]$ , then there is a mapping  $\tau : [n]^2 \rightarrow [n]$  such that, for all  $i, j$  we have  $H_{i,*} \bullet H_{j,*} = H_{\tau(i,j),*}$ . Fix an arbitrary  $j \in [n]$  and consider the map  $\tau_j := \tau(\cdot, j)$ . This map is bijective. To see this, assume that  $\tau(a, j) = \tau(c, j)$ , which implies that  $H_{a,*} \bullet H_{j,*} = H_{c,*} \bullet H_{j,*}$  which yields  $H_a = H_c$ . Therefore, we see that, for all  $i, j \in [n]$  there is a  $c \in [n]$  such that  $\tau(c, j) = i$ , that is,  $H_{c,*} \bullet H_{j,*} = H_{i,*}$  which yields  $H_{i,*} \circ H_{j,*} = H_{c,*}$ . Since  $H$  is Hermitian this also proves the second part of the group condition.  $\dashv$

Assume that there are  $a', b' \in [n]$  such that  $H_{a',*} \bullet H_{b',*} \notin R(H)$ . Fix such  $a', b'$  and let  $i = 1$  then we have

$$C_{1j}^{[q]} = \sum_{a=1}^n \sum_{b=1}^n |\langle H_{a,*} \bullet H_{b,*}, H_{j,*} \bullet H_{1,*} \rangle|^{2q} = \sum_{a=1}^n \sum_{b=1}^n |\langle H_{a,*} \bullet H_{b,*}, H_{j,*} \rangle|^{2q}$$

Note that for all  $a, b$  we have  $|\langle H_{a,*} \bullet H_{b,*}, H_{j,*} \rangle| \leq n$  and further

*Claim 2.*  $|\langle H_{a',*} \bullet H_{b',*}, H_{j,*} \rangle| < n$  for all  $j \in [n]$ .

*Proof.* Assume that  $|\langle H_{a',*} \bullet H_{b',*}, H_{j,*} \rangle| = n$ . Then the Cauchy-Schwarz inequality implies that there is a  $\zeta$  such that  $H_{a',*} \bullet H_{b',*} = \zeta H_{j,*}$  but as  $H$  is normalized we have  $H_{j1} = (H_{a',*} \bullet H_{b',*})_1 = 1$  and therefore  $\zeta = 1$  which implies  $H_{a',*} \bullet H_{b',*} \in R(H)$  in contradiction to our assumption.  $\dashv$

*Claim 3.* There is a  $j \in [n]$  such that  $\langle H_{a',*} \bullet H_{b',*}, H_{j,*} \rangle \neq 0$ .

*Proof.* Otherwise,  $H_{a',*} \bullet H_{b',*}$  would be orthogonal to all vectors in  $R(H)$  and by  $H_{a',*} \bullet H_{b',*} \notin R(H)$  this would imply an  $n+1$  element basis of an  $n$ -dimensional vector space.  $\dashv$

By construction we have  $\text{abs}(C^{[q]}) = C^{[q]}$  and  $C^{[q]}$  is symmetric for all  $q$ . Therefore the proof follows from Lemma 4.23 if we can show that there is a  $j \in [n]$  such that the  $2 \times 2$  submatrix of  $C^{[q]}$  induced by  $1, j$  is indecomposable and has rank 2. We have  $C_{ii}^{[q]} = n^{2q+1}$  for all  $i \in [n]$ , as

$$C_{ii}^{[q]} = \sum_{a=1}^n \sum_{b=1}^n |\langle H_{a,*} \bullet H_{b,*}, H_{i,*} \bullet H_{i,*} \rangle|^{2q} = \sum_{a=1}^n \sum_{b=1}^n |\langle H_{a,*}, H_{b,*} \rangle|^{2q}$$

and the term  $|\langle H_{a,*}, H_{b,*} \rangle|$  is non-zero iff  $a = b$ . Fix  $j \in [n]$  as in Claim 3. We see that the  $2 \times 2$  submatrix of  $C^{[q]}$  induced by  $1, j$  satisfies

$$\begin{pmatrix} C_{11}^{[q]} & C_{1j}^{[q]} \\ C_{j1}^{[q]} & C_{jj}^{[q]} \end{pmatrix} = \begin{pmatrix} n^{2q+1} & C_{1j}^{[q]} \\ C_{j1}^{[q]} & n^{2q+1} \end{pmatrix}.$$

Claim 3 further implies that it is indecomposable. To show that this submatrix is a witness of a block of rank at least 2 it remains to show that its determinant  $n^{4q+2} - (C_{1j}^{[q]})^2$  is non-zero for some  $q$ . Define values  $c_0, \dots, c_n$  by  $c_\nu = |\{(a, b) \in [n]^2 : |\langle H_{a,*} \bullet H_{b,*}, H_{j,*} \rangle| = \nu\}|$ . Then we can rewrite

$$C_{1j}^{[q]} = \sum_{a=1}^n \sum_{b=1}^n |\langle H_{a,*} \bullet H_{b,*}, H_{j,*} \rangle|^{2q} = \sum_{\nu=1}^n c_\nu \nu^{2q}$$

Assume, for contradiction that the above mentioned determinant is zero for all  $q$ . This implies that

$$C_{1j}^{[q]} = n^{2q+1} = \sum_{\nu=0}^n c'_\nu \nu^{2q}$$

for  $c'_0, \dots, c'_n$  such that  $c'_0 = c'_{n-1} = 0$  and  $c'_n = n$ . By Lemma 4.4 we see that for some large enough computable  $q$  this implies that  $c_\nu = c'_\nu$  for all  $\nu \in [n]$ . In particular  $n = c'_n = c_n$  which contradicts the fact that Claim 2 implies  $c_n = 0$ .  $\square$

## 6.2 The Representation Conditions (R1) through (R5)

Now we shall describe how to satisfy the Representation Conditions (R1)–(R5).

**Lemma 6.4.** *Let  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  be an (H-STD) problem such that  $H$  and  $\mathbf{D}$  satisfy (R1)–(R2). Then  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is #P-hard unless conditions (R3) and (R4) are satisfied.*

*Proof.* Fix some  $c \in \mathbb{Z}_\omega$ , we may assume that  $c > 0$  as for  $c = 0$  we have  $\beta_0 = 0$  and  $\mathfrak{G}_0 = \mathfrak{G}$  by the fact that  $D^{\llbracket 0 \rrbracket} = I_n$ . Further, for  $-c > 0$  we know that  $\overline{D}^{\llbracket c \rrbracket} = D^{\llbracket -c \rrbracket}$  by (H-STD) and thus  $\Lambda_c = \Lambda_{-c}$ .

For any  $c > 0$  we will construct a reduction as follows. Let  $G = (V, E)$  be a given digraph and  $\phi$  a pinning. We construct a digraph  $G^c$  from  $G$  by replacing each edge  $e = uv$  by a distinct length 2 path and call the middle vertex of this path  $v_e$ . Then we add another vertex  $v'_e$  to the graph and connect  $v_e$  to  $v'_e$  (in this direction) by  $c$  distinct length 2 paths. Formally, we have  $G^c = (V^c, E^c)$  with

$$\begin{aligned} V^c &= V \cup \{v_e, v'_e, v_{e,1}, \dots, v_{e,c} \mid e \in E\} \\ E^c &= \{v_e v_{e,i}, v_{e,i} v'_e \mid i \in [c], e \in E\} \end{aligned}$$

We have  $c = \partial(v_e) = -\partial(v'_e)$  and therefore the vertex weights of  $v_e$  and  $v'_e$  have the same support  $\Lambda_c$ . The above construction witnesses a reduction  $\text{EVAL}^{\text{pin}}(C, \mathbf{D}) \leq \text{EVAL}^{\text{pin}}(H, \mathbf{D})$  for a matrix  $C$  which we will describe now. We label the rows and columns of  $C$  symmetrically by the elements of  $\mathfrak{G}$ . Let  $a, b, g, h \in \mathfrak{G}$  denote the spins of  $u, v, v_e$  and  $v'_e$  respectively. Then

$$\begin{aligned} C_{a,b} &= \sum_{g \in \mathfrak{G}} H_{a,-g} H_{g,-b} D_{g,g}^{\llbracket c \rrbracket} \sum_{h \in \mathfrak{G}} D_{h,h}^{\llbracket -c \rrbracket} \left( \sum_{\mu \in \mathfrak{G}} H_{g,-\mu} H_{\mu,-h} D_{\mu,\mu}^{\llbracket 0 \rrbracket} \right)^c \\ &= \sum_{g,h \in \Lambda_c} H_{a,-g} \overline{H_{b,-g}} \overline{D_{g,g}^{\llbracket c \rrbracket}} \overline{D_{h,h}^{\llbracket c \rrbracket}} \langle H_{g,*}, H_{h,*} \rangle^c \end{aligned}$$

The second equality follows from the fact that  $D^{[0]} = I_n$  and  $H_{\mu, -h} = \overline{H}_{h, -\mu}$ . We know that  $\langle H_{g,*}, H_{h,*} \rangle = 0$  unless  $g = h$ . And if  $g = h$ , then  $\langle H_{g,*}, H_{h,*} \rangle = n$ . Thus, we have

$$C_{a,b} = \sum_{g \in \Lambda_c} H_{a,-g} \overline{H}_{b,-g} D_{g,g}^{[c]} \overline{D_{g,g}^{[c]}} n^c = n^c \sum_{g \in \Lambda_c} H_{b,g} \overline{H}_{a,g}.$$

Note that the right equality uses  $H_{a,-g} = \overline{H}_{a,g}$ . We know that  $\Lambda_c \subseteq \mathfrak{G}$  but it might be the case that the neutral element 0 of  $\mathfrak{G}$  is not contained in  $\Lambda_c$ . Fix some  $\lambda \in \Lambda_c$  and define  $S = \{g - \lambda \mid g \in \Lambda_c\}$  which clearly contains 0. We have

$$C_{ab} = n^c \sum_{g \in \Lambda_c} H_{b-a,g} = n^c \sum_{x \in S} H_{b-a,x+\lambda} = n^c H_{b-a,\lambda} \cdot \sum_{x \in S} H_{b-a,x} \quad (59)$$

Let  $\chi : \mathfrak{G} \rightarrow \{0, 1\}$  denote the characteristic function of  $S$ , then row 0 of  $C$  satisfies

$$C_{0b} = n^c H_{b,\lambda} \sum_{x \in \mathfrak{G}} H_{b,x} \chi(x) = n^c H_{b,\lambda} \langle H_{b,*}, \chi \rangle.$$

Define  $\mathcal{C}_0 = \{b \in \mathfrak{G} \mid \langle b, g \rangle_\omega = 0 \text{ for all } g \in S\}$  and recall that  $\mathcal{X}[0] = 1$ . Thus

$$\langle H_{b,*}, \chi \rangle = \sum_{g \in S} \mathcal{X}[\langle b, -g \rangle_\omega] = \sum_{g \in S} \mathcal{X}[-\langle b, g \rangle_\omega] = \sum_{g \in S} \mathcal{X}[0] = |S| \quad \text{for all } b \in \mathcal{C}_0. \quad (60)$$

*Claim 1.* If  $\text{EVAL}(C, \mathbf{D})$  is not  $\#P$ -hard then for all  $b \in \mathfrak{G} \setminus \mathcal{C}_0$  we have  $\langle H_{b,*}, \chi \rangle = 0$ .

*Proof.* Fix an element  $b \in \mathfrak{G} \setminus \mathcal{C}_0$ . Equation (59) straightforwardly implies that  $C_{aa} = n^c |S|$  for all  $a \in \mathfrak{G}$ . Consider a  $2 \times 2$  submatrix of  $\text{abs}(C)$  induced by 0 and  $b$ ,

$$\begin{pmatrix} |C_{00}| & |C_{0b}| \\ |C_{b0}| & |C_{bb}| \end{pmatrix} = n^c \cdot \begin{pmatrix} |S| & |\langle H_{b,*}, \chi \rangle| \\ |\langle H_{b,*}, \chi \rangle| & |S| \end{pmatrix}.$$

By Lemma 4.23 the problem  $\text{EVAL}^{\text{pin}}(C, \mathbf{D})$  is  $\#P$ -hard, if  $\text{abs}(C)$  contains a block of row rank at least 2. Therefore no such  $2 \times 2$  submatrix can be a witness for the existence of a block of rank at least 2 in  $\text{abs}(C)$ . This however is possible only if either  $|\langle H_{b,*}, \chi \rangle| = 0$  or the determinant of this submatrix is zero. The latter would imply  $|S| = |\langle H_{b,*}, \chi \rangle|$  which is impossible for the following reasons. First of all, as  $H$  is normalized, and  $0 \in S$  the expression  $\langle H_{b,*}, \chi \rangle = \sum_{x \in S} H_{b,x}$  contains at least one 1 entry. However, as  $b \notin \mathcal{C}_0$  we see that  $H_{b,*} = \mathcal{X}[\langle b, * \rangle_\omega]$  is not constantly 1 on  $S$  which implies  $|\langle H_{b,*}, \chi \rangle| < |S|$  and the claim follows.  $\dashv$

Define  $\mathfrak{S}$  as the smallest subgroup of  $\mathfrak{G}$  containing  $S$ . Recall that by the subgroup criterion of finite groups, each element of  $\mathfrak{S}$  is of the form  $\sum_{g \in S} \lambda_g g$  for appropriate  $\lambda_g \in \mathbb{Z}$ . Thus for every  $b \in \mathcal{C}_0$  and every  $g' \in \mathfrak{S}$  we have  $\langle b, g' \rangle_\omega = \langle b, \left(\sum_{g \in S} \lambda_g g\right) \rangle_\omega = \sum_{g \in S} \lambda_g \langle b, g \rangle_\omega = 0$ .

Let  $\chi_{\mathfrak{S}} : \mathfrak{G} \rightarrow \{0, 1\}$  be the characteristic function of  $\mathfrak{S}$ . Analogously to the above we see that for all  $b \in \mathcal{C}_0$ ,

$$\langle H_{b,*}, \chi_{\mathfrak{S}} \rangle = \sum_{g' \in \mathfrak{S}} \mathcal{X}[-\langle b, g' \rangle_\omega] = \sum_{g' \in \mathfrak{S}} \mathcal{X}\left[-\sum_{g \in S} \lambda_g \langle b, g \rangle_\omega\right] = \sum_{g' \in \mathfrak{S}} \mathcal{X}[0] = |\mathfrak{S}|. \quad (61)$$

We will furthermore see that

*Claim 2.* For all  $b \in \mathfrak{G} \setminus \mathcal{C}_0$  we have  $\langle H_{b,*}, \chi_{\mathfrak{S}} \rangle = 0$ .

Before we prove this claim we will argue that this finishes the proof of the lemma. Note first that, the basic properties of Fourier analysis of Abelian groups imply that

$$\chi(x) = \frac{1}{|\mathfrak{G}|} \sum_{g \in \mathfrak{G}} \langle H_{g,*}, \chi \rangle \cdot \overline{H}_{g,x}.$$

and

$$\chi_{\mathfrak{S}}(x) = \frac{1}{|\mathfrak{S}|} \sum_{g \in \mathfrak{S}} \langle H_{g,*}, \chi_{\mathfrak{S}} \rangle \cdot \overline{H}_{g,x}.$$

Combining Claims 1 and 2 and equations (60) and (61) we see that for all  $g \in \mathfrak{G}$  we have  $\langle H_{g,*}, \chi_{\mathfrak{S}} \rangle |S| = \langle H_{g,*}, \chi \rangle |\mathfrak{S}|$ . Which implies that  $\chi(x) |\mathfrak{S}| = \chi_{\mathfrak{S}}(x) |S|$  for all  $x \in \mathfrak{G}$ , that is  $\mathfrak{S} = S$ . It follows straightforwardly that  $\Lambda_c = \lambda + \mathfrak{S}$ . That is, it is a coset of  $\mathfrak{S}$ . This proves condition **(R3)**. Recall then from the discussion of conditions **(R1)** through **(R5)** in Section 3.3 that condition **(R4)** is satisfied, as well. This finishes the proof.

**The Proof of Claim 2.** Let  $b \in \mathfrak{G} \setminus \mathcal{C}_0$  and define  $\mathfrak{S}_{\alpha}^b = \{g \in \mathfrak{S} \mid \langle b, g \rangle_{\omega} = \alpha\}$  for all  $\alpha \in \mathbb{Z}_{\omega}$ . As  $\langle b, * \rangle_{\omega}$  defines a homomorphism, each nonempty set  $\mathfrak{S}_{\alpha}^b$  is just a fiber of this homomorphism and  $\mathfrak{S}_0^b$  is its kernel. In particular,  $\mathfrak{S}_0^b$  is a subgroup of  $\mathfrak{S}$ , it is non-empty as  $0 \in \mathfrak{S}_0^b$  and the other non-empty sets  $\mathfrak{S}_{\alpha}^b$  are its cosets.

Let  $\mathfrak{A} = \{\alpha \in \mathbb{Z}_{\omega} \mid \mathfrak{S}_{\alpha}^b \neq \emptyset\}$  be the subset of  $\mathbb{Z}_{\omega}$  which selects all non-empty  $\mathfrak{S}_{\alpha}^b$ . The set  $\mathfrak{A}$  is an Abelian group. To see this, recall that  $0 \in \mathfrak{A}$  and further the existence of elements  $g \in \mathfrak{S}_{\alpha}^b$  and  $h \in \mathfrak{S}_{\alpha'}^b$  denotes  $\langle b, g \rangle_{\omega} = \alpha$  and  $\langle b, h \rangle_{\omega} = \alpha'$ . We have  $g + h \in \mathfrak{S}$  and by the bilinearity of the  $\langle *, * \rangle_{\omega}$  operator  $\alpha + \alpha' = \langle b, g \rangle_{\omega} + \langle b, h \rangle_{\omega} = \langle b, g + h \rangle_{\omega}$ . Thus  $\mathfrak{S}_{\alpha+\alpha'}^b$  is non-empty and therefore the subgroup criterion implies that  $\mathfrak{A}$  is a group. We have

$$\langle H_{b,*}, \chi_{\mathfrak{S}} \rangle = \sum_{g \in \mathfrak{S}} \mathcal{X}[\langle b, -g \rangle_{\omega}] = \sum_{\alpha \in \mathfrak{A}} \sum_{\substack{g \in \mathfrak{S} \\ \langle b, g \rangle_{\omega} = -\alpha}} \mathcal{X}[\alpha] = \sum_{\alpha \in \mathfrak{A}} \mathcal{X}[\alpha] \cdot |\mathfrak{S}_{-\alpha}^b|$$

As the  $\mathfrak{S}_{\alpha}^b$  are cosets of  $\mathfrak{S}_0^b$  they all have the same cardinality and we obtain

$$\langle H_{b,*}, \chi_{\mathfrak{S}} \rangle = |\mathfrak{S}_0^b| \cdot \sum_{\alpha \in \mathfrak{A}} \mathcal{X}[\alpha].$$

It remains to show that the right hand side sum is zero. By the Fundamental Theorem of Finitely Generated Abelian Groups, there is a direct sum decomposition  $\mathfrak{A} \cong \mathfrak{C}_1 \oplus \dots \oplus \mathfrak{C}_z$  and each of these cyclic groups has all elements of the form  $\lambda_i h_i$  for some  $\lambda_i \in \mathbb{Z}_{\text{ord}(h_i)}$  and  $h_i$  for  $i \in [z]$ . Therefore,

$$\sum_{\alpha \in \mathfrak{A}} \mathcal{X}[\alpha] = \sum_{\lambda_1 \in \mathbb{Z}_{\text{ord}(h_1)}} \dots \sum_{\lambda_z \in \mathbb{Z}_{\text{ord}(h_z)}} \prod_{i=1}^z \mathcal{X}[h_i]^{\lambda_i} = \prod_{i=1}^z \sum_{\lambda_i \in \mathbb{Z}_{\text{ord}(h_i)}} \mathcal{X}[h_i]^{\lambda_i} \quad (62)$$

And each of the sums on the right hand side satisfies

$$\sum_{\lambda_i \in \mathbb{Z}_{\text{ord}(h_i)}} \mathcal{X}[h_i]^{\lambda_i} = 0$$



provided that  $h_i \neq 0$ , as  $\mathcal{X}[h_i]$  is some  $\text{ord}(h_i)$ -th root of unity. Further, since  $b \in \mathfrak{G} \setminus \mathcal{C}_0$  there is at least one element in  $\mathfrak{A}$  which is not the neutral element. Therefore in the decomposition of  $\mathfrak{A}$  at least one non-trivial generator  $h_i \neq 0$  exists. This proves that the term in equation (62) is zero and thus finishes the proof of the claim.  $\square$

**Lemma 6.5.** *Let  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  be an (H-STD) problem such that  $H$  satisfies (GC). Assume that  $H$  and  $\mathbf{D}$  have a representation as given in (R1)–(R4). There is an (H-STD)-problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D}')$  which satisfies conditions (R1)–(R5) such that*

$$\text{EVAL}^{\text{pin}}(H, \mathbf{D}) \equiv \text{EVAL}^{\text{pin}}(H, \mathbf{D}').$$

*Proof.* Define, for each  $c \in \mathbb{Z}_\omega$  values  $\lambda_c$  as follows. If  $D^{\llbracket c \rrbracket} = 0$  let  $\lambda_c = 0$ . Otherwise, we know by condition (R4) that  $D_{\beta_c, \beta_c}^{\llbracket c \rrbracket} = \mathcal{X}[\rho_c(0)]$ . We define  $\lambda_c = \mathcal{X}[\rho_c(0)]^{-1}$  and let  $\mathbf{D}' = (\lambda_c \cdot D^{\llbracket c \rrbracket})_{c \in \mathbb{Z}_\omega}$ . Let  $G = (V, E)$  be a digraph and  $\phi$  a pinning. Let, for each  $c \in \mathbb{Z}_\omega$  be  $n_c$  the number of vertices  $v \in V \setminus \text{def}(\phi)$  such that  $\llbracket \partial(v) \rrbracket = c$ . Then

$$Z_{H, \mathbf{D}}(\phi, G) = \left( \prod_{c=0}^{\omega-1} \lambda_c^{n_c} \right) Z_{H, \mathbf{D}'}(\phi, G).$$

This proves the reducibility in both directions.  $\square$

### 6.3 The Affinity Condition (AF)

In the present situation we are faced with an (H-STD) problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  which already satisfies the group condition (GC) and the representability conditions (R1)–(R5). Our aim will be now to provide the last big step necessary for proving Lemma 6.1. This step is given by the following Lemma.

**Lemma 6.6 (The Non-Bipartite Affinity Lemma).** *Let  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  be some (H-STD)-problem such that  $H$  satisfies (GC). Assume that  $H$  and  $\mathbf{D}$  have a representation as given in (R1)–(R5). If (AF) is not satisfied then  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is #P-hard.*

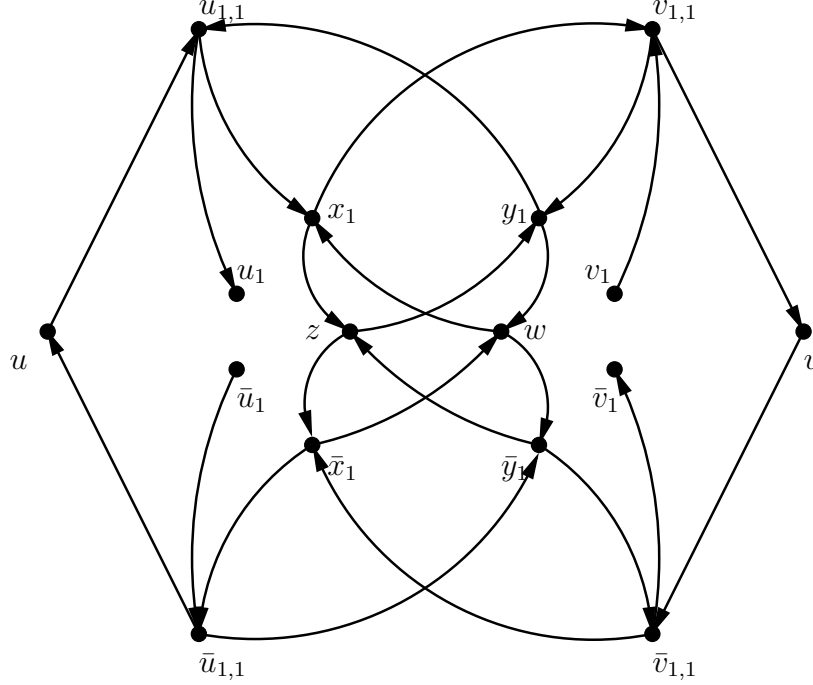
The proof relies on a construction which we will analyze separately in Lemma 6.7 so as to make it more digestible. We shall describe the reduction first.

**The Nymphaea Reduction.** We consider the problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  as above. Let  $G = (V, E)$  be a given digraph and  $\phi$  a pinning. For parameters  $p$  and  $q$ , we construct a digraph  $G' = G'(p, q)$  by replacing each edge in  $G$  by a graph  $\Gamma_{p,q}$  which has two distinguished terminals  $u$  and  $v$ . We refer to this graph as the "Nymphaea" (see Figure 3). The vertex set of  $\Gamma_{p,q}$  is

$$\{u, v, z, w, u_{i,j}, \bar{u}_{i,j}, u_i, \bar{u}_i, v_{i,j}, \bar{v}_{i,j}, v_i, \bar{v}_i, x_i, \bar{x}_i, y_i, \bar{y}_i \mid i \in [p], j \in [q]\} \quad (63)$$

Its edge set is

$$\begin{aligned} & \{uu_{i,j}, y_i u_{i,j}, u_{i,j} u_i, u_{i,j} x_i \mid i \in [p], j \in [q]\} \cup \{ \bar{u}_{i,j} u, \bar{u}_{i,j} \bar{y}_i, \bar{u}_i \bar{u}_{i,j}, \bar{x}_i \bar{u}_{i,j} \mid i \in [p], j \in [q] \} \\ \cup & \{v_{i,j} v, v_{i,j} y_i, v_{i,j} v_{i,j}, x_i v_{i,j} \mid i \in [p], j \in [q]\} \cup \{v \bar{v}_{i,j}, \bar{y}_i \bar{v}_{i,j}, \bar{v}_i \bar{v}_{i,j}, \bar{v}_{i,j} \bar{x}_i \mid i \in [p], j \in [q]\} \\ \cup & \{x_i z, w x_i, z y_i, y_i w \mid i \in [p], j \in [q]\} \cup \{z \bar{x}_i, \bar{x}_i w, \bar{y}_i z, w \bar{y}_i \mid i \in [p], j \in [q]\} \end{aligned} \quad (64)$$

Figure 3: Nymphaea for  $p = 1, q = 1$ 

**Lemma 6.7.** *Let  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  be an **(H-STD)** problem such that  $H$  satisfies **(GC)**. Assume that  $H$  and  $\mathbf{D}$  have a representation as given in **(R1)**–**(R4)**.*

*Then for all  $p \in \mathbb{N}$  and  $q \in \mathbb{Z}_\omega$  the Nymphaea reduction witnesses*

$$\text{EVAL}^{\text{pin}}(C) \leq \text{EVAL}^{\text{pin}}(H, \mathbf{D})$$

*for a non-negative real valued  $n \times n$  matrix  $C = C(p, q)$  which satisfies the following. For all  $u, v \in \beta_q + \mathfrak{G}_q$  we have*

$$C_{u,v} = \sum_{g \in \mathfrak{G}} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(v - \beta_q + x) - \rho_q(u - \beta_q + x) + \langle g, x \rangle_\omega] \right|^{2p}$$

*Proof.* Let  $G = (V, E)$  be a digraph and  $\phi$  a pinning. For parameters  $p$  and  $q$  let  $G' = G'(p, q)$  by the digraph of the Nymphaea reduction as described above.

Observe first that there is a certain axis of symmetry in the Nymphaea which has also been made explicit in Figure 3. The vertices  $u, v, z, w$  lie on this axis and all other vertices occur in two forms, without the bar (e.g.  $u_i$ ) and with the bar ( $\bar{u}_i$ ). Further, the connections of the unbarred vertices are the same as for the barred ones except for the fact that the directions are reversed. By  $H$  being Hermitian, this amounts to a conjugation of the corresponding contributions and will become important in the following. First of all, due to this symmetry, it will suffice to analyze the unbarred part of the gadget. The results for the barred part then follow clearly by conjugation.

**Analyzing the Nymphaea.** To simplify the analysis further we will focus on one of its subgraphs first. For some  $i \in [p]$ ,  $j \in [q]$  consider the subgraph induced by vertices  $u, u_{i,j}, u_i, x_i, y_i$ . We will fix the spins of  $u, u_i, x_i$ , and  $y_i$  for the moment and — slightly abusing notation — denote these by just the vertices they correspond to. We denote the contribution of this subgraph excluding the vertex weights of  $u, u_i, x_i, y_i$  by  $Z_1(u, u_i, x_i, y_i)$ . The vertex  $u_{i,j}$  will not be fixed and its spin will be denoted by  $\mu$ . Note that  $\partial(u_{i,j}) = 0$  which implies by **(H-STD)** that the vertex weights on  $u_{i,j}$  are inessential. Then — recall that  $H$  is indexed by elements of the group  $\mathfrak{G}$  — it follows that

$$\begin{aligned} Z_1(u, u_i, x_i, y_i) &= \sum_{\mu \in \mathfrak{G}} H_{u, -\mu} H_{\mu, -x_i} H_{y_i, -\mu} H_{\mu, -u_i} \\ &= \sum_{\mu \in \mathfrak{G}} H_{u, -\mu} \overline{H}_{x_i, -\mu} H_{y_i, -\mu} \overline{H}_{u_i, -\mu} \\ &= \sum_{\mu \in \mathfrak{G}} H_{u-x_i+y_i-u_i, -\mu} \end{aligned}$$

This can be rephrased as  $Z_1(u, u_i, x_i, y_i) = \langle H_{u-x_i+y_i-u_i, *}, H_{0, *} \rangle$  which by the Hadamard property of  $H$  implies that  $Z_1(u, u_i, x_i, y_i) = 0$  unless  $u - x_i + y_i - u_i = 0$  and if so, we have  $Z_1(u, u_i, x_i, y_i) = n$ .

Analogous reasoning on the subgraph induced by vertices  $v, v_{i,j}, v_i, x_i, y_i$  shows that its contribution is

$$Z_2(v, v_i, x_i, y_i) = \langle H_{v_i-v+x_i-y_i, *}, H_{0, *} \rangle.$$

Similarly, this is zero unless  $v_i - v + x_i - y_i = 0$ , and if so we have  $Z_2(v, v_i, x_i, y_i) = n$ .

Let now  $Z_1^q(u, u_i, x_i, y_i)$  denote the contribution of the subgraph defined by  $u, u_{i,j}, u_i, x_i, y_i$  for all  $j \in [q]$ . Then straightforwardly  $Z_1^q(u, u_i, x_i, y_i) = Z_1(u, u_i, x_i, y_i)^q$ . Defining  $Z_2^q(v, v_i, x_i, y_i)$  analogously on  $v, v_{i,j}, v_i, x_i, y_i$  for all  $j \in [q]$  we obtain  $Z_2^q(v, v_i, x_i, y_i) = Z_2(v, v_i, x_i, y_i)^q$ . Furthermore, for the subgraph on vertices  $z, w, x_i, y_i$  we have a contribution of

$$H_{x_i, -z} H_{z, -y_i} H_{w, -x_i} H_{y_i, -w} = H_{x_i, -z} \overline{H}_{y_i, -z} \overline{H}_{x_i, -w} H_{y_i, -w} = \mathcal{X}[\langle x_i - y_i, z - w \rangle_\omega]$$

Let us now turn to the complete gadget. Note that  $0 = \partial(z) = \partial(w) = 0$  and  $\partial(x_i) = \partial(y_i) = 0$  for all  $i \in [q]$ . Therefore the corresponding vertex weights are inessential. The remaining vertices  $u_i, v_i$  satisfy  $-\partial(u_i) = \partial(v_i) = q$ . By condition **(H-STD)** we know that  $D^{\llbracket -q \rrbracket} = \overline{D^{\llbracket q \rrbracket}}$  which particularly implies that the support of these two is the same, namely  $\Lambda_q = \Lambda_{-q}$ . Let  $\mu, \nu$  be the spins of  $u_i$  and  $v_i$  respectively. For every fixed  $i \in [p]$  and every configuration of  $u, v, x_i, y_i$  the subgraph defined by  $u, v, x_i, y_i, u_i, v_i, u_{i,j}, v_{i,j}$  for all  $j \in [q]$  then yields a contribution

$$Z(u, v, x_i, y_i) = \sum_{\mu, \nu \in \Lambda_q} \overline{D_{\mu, \mu}^{\llbracket q \rrbracket}} D_{\nu, \nu}^{\llbracket q \rrbracket} Z_1(u, \mu, x_i, y_i)^q Z_2(v, \nu, x_i, y_i)^q$$

and by the above reasoning on  $Z_1$  and  $Z_2$  we have

$$Z(u, v, x_i, y_i) = \sum_{\mu, \nu \in \Lambda_q} \overline{D_{\mu, \mu}^{\llbracket q \rrbracket}} D_{\nu, \nu}^{\llbracket q \rrbracket} \langle H_{u-x_i+y_i-\mu, *}, H_{0, *} \rangle^q \langle H_{v-v+x_i-y_i, *}, H_{0, *} \rangle^q \quad (65)$$

$$= n^{2q} \overline{D_{u-x_i+y_i, u-x_i+y_i}^{\llbracket q \rrbracket}} D_{v-x_i+y_i, v-x_i+y_i}^{\llbracket q \rrbracket} \quad (66)$$

where we now included all vertex weights. By the fact that the bared part of the Nymphaea has all edges in reverse direction we obtain by the same arguments as above that

$$H_{z,-\bar{x}_i} H_{\bar{y}_i,-z} H_{\bar{x}_i,-w} H_{w,-\bar{y}_i} = \overline{\mathcal{X}[\langle \bar{x}_i - \bar{y}_i, z - w \rangle_\omega]}$$

Further the the subgraph defined by  $u, v, \bar{x}_i, \bar{y}_i, \bar{u}_i, \bar{v}_i, \bar{u}_{i,j}, \bar{v}_{i,j}$  for all  $j \in [q]$  then yields a contribution

$$\bar{Z}(u, v, \bar{x}_i, \bar{y}_i) = \sum_{\mu, \nu \in \Lambda_q} D_{\mu, \mu}^{[q]} \overline{D_{\nu, \nu}^{[q]} \langle H_{u-\bar{x}_i+\bar{y}_i-\mu, *}, H_{0, *} \rangle^q \langle H_{\nu-v+\bar{x}_i-\bar{y}_i, *}, H_{0, *} \rangle^q}$$

That is

$$\bar{Z}(u, v, \bar{x}_i, \bar{y}_i) = \overline{Z(u, v, \bar{x}_i, \bar{y}_i)} \quad (67)$$

Note further, that by construction all original vertices have grade 0. Altogether, the Nymphaea therefore witnesses a reduction  $\text{EVAL}^{\text{pin}}(C') \leq \text{EVAL}^{\text{pin}}(H, \mathbf{D})$  for a symmetric non-negative matrix  $C'$  defined by

$$\begin{aligned} C'_{u,v} &= \sum_{z, w \in \mathfrak{G}} \prod_{i=1}^p \left( \sum_{x_i, y_i \in \mathfrak{G}} Z(u, v, x_i, y_i) \mathcal{X}[\langle x_i - y_i, z - w \rangle_\omega] \right) \\ &\quad \times \prod_{i=1}^p \left( \sum_{\bar{x}_i, \bar{y}_i \in \mathfrak{G}} \bar{Z}(u, v, \bar{x}_i, \bar{y}_i) \overline{\mathcal{X}[\langle \bar{x}_i - \bar{y}_i, z - w \rangle_\omega]} \right) \end{aligned}$$

Furthermore as the different parts of the  $p$ -adic product terms in the definition of  $C'$  are all independent, we can replace all  $x_i, \bar{x}_i$  and  $y_i, \bar{y}_i$  by only two variables  $x, y$ . By application of equation (67) we obtain

$$\begin{aligned} C'_{u,v} &= \sum_{z, w \in \mathfrak{G}} \prod_{i=1}^p \left( \sum_{x, y \in \mathfrak{G}} Z(u, v, x, y) \mathcal{X}[\langle x - y, z - w \rangle_\omega] \right) \\ &\quad \times \prod_{i=1}^p \left( \overline{\sum_{x, y \in \mathfrak{G}} Z(u, v, x, y) \mathcal{X}[\langle x - y, z - w \rangle_\omega]} \right) \\ &= \sum_{z, w \in \mathfrak{G}} \left| \sum_{x, y \in \mathfrak{G}} Z(u, v, x, y) \mathcal{X}[\langle x - y, z - w \rangle_\omega] \right|^{2p} \end{aligned}$$

Note that for all  $z, g \in \mathfrak{G}$  the equation  $z - w = g$  has a unique solution  $w \in \mathfrak{G}$ . Therefore we can simplify

$$C'_{u,v} = n \sum_{g \in \mathfrak{G}} \left| \sum_{x, y \in \mathfrak{G}} Z(u, v, x, y) \mathcal{X}[\langle x - y, g \rangle_\omega] \right|^{2p}$$

And with the definition of  $Z(u, v, x, y)$  as given in equation (66) we get

$$C'_{u,v} = n \sum_{g \in \mathfrak{G}} \left| \sum_{x, y \in \mathfrak{G}} n^{2q} \overline{D_{u-x+y, u-x+y}^{[q]} D_{v-x+y, v-x+y}^{[q]} \mathcal{X}[\langle x - y, g \rangle_\omega]} \right|^{2p}$$

Now, for all  $x, a \in \mathfrak{G}$  there is an unique solution  $y$  to the equation  $x - y = a$ . Thus

$$\begin{aligned} C'_{u,v} &= n^{4pq+1} \sum_{g \in \mathfrak{G}} \left| n \sum_{x \in \mathfrak{G}} \overline{D_{u-x, u-x}^{[q]}} D_{v-x, v-x}^{[q]} \cdot \mathcal{X}[\langle x, g \rangle_\omega] \right|^{2p} \\ &= n^{4pq+2p+1} \sum_{g \in \mathfrak{G}} \left| \sum_{x \in \mathfrak{G}} \overline{D_{u-x, u-x}^{[q]}} D_{v-x, v-x}^{[q]} \cdot \mathcal{X}[\langle x, g \rangle_\omega] \right|^{2p} \end{aligned}$$

Defining  $C = n^{-(4pq+2p+1)} \cdot C'$  we have  $\text{EVAL}^{\text{pin}}(C) \equiv \text{EVAL}^{\text{pin}}(C')$ . We will show that  $C$  satisfies the statement of the lemma. By condition **(R3)** we have  $\Lambda_q = \beta_q + \mathfrak{G}_q$  for some  $\beta_q \in \mathfrak{G}$  and  $\mathfrak{G}_q$  a subgroup of  $\mathfrak{G}$ . In the following we will make the additional assumption that  $u - \beta_q, v - \beta_q \in \mathfrak{G}_q$ . Recall that the vertex weights  $\overline{D_{u-x, u-x}^{[q]}} D_{v-x, v-x}^{[q]}$  are non-zero iff  $v - x, u - x \in \Lambda_q$ . This thus is satisfied iff  $x \in \mathfrak{G}_q$  and we may rewrite

$$\begin{aligned} C_{u,v} &= \sum_{g \in \mathfrak{G}} \left| \sum_{x \in \mathfrak{G}_q} \overline{D_{u-x, u-x}^{[q]}} D_{v-x, v-x}^{[q]} \cdot \mathcal{X}[\langle x, g \rangle_\omega] \right|^{2p} \\ &= \sum_{g \in \mathfrak{G}} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X}[\rho_q(v - \beta_q - x) - \rho_q(u - \beta_q - x) + \langle g, -x \rangle_\omega] \right|^{2p} \\ &= \sum_{g \in \mathfrak{G}} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X}[\rho_q(v - \beta_q + x) - \rho_q(u - \beta_q + x) + \langle g, x \rangle_\omega] \right|^{2p} \end{aligned}$$

where the second equality follows from the group theoretic definition of  $D^{[q]}$  as given in **(R4)** and from the skew-bilinearity:  $\langle x, g \rangle_\omega = -\langle g, x \rangle_\omega = \langle g, -x \rangle_\omega$ . The last equality follows from the fact that we are summing over all  $x \in \mathfrak{G}_q$  which renders the inversion  $-x$  of  $x$  irrelevant.  $\square$

We are now in a position to prove the Non-Bipartite Affinity Lemma 6.6.

*Proof (of Lemma 6.6).* Fix some  $q \in \mathbb{Z}_\omega$  such that  $q \geq 0$ . For every  $p \in \mathbb{N}$  Lemma 6.7 just proved shows that the Nymphaea reduction witnesses

$$\text{EVAL}^{\text{pin}}(C) \leq \text{EVAL}^{\text{pin}}(H, \mathbf{D})$$

for a non-negative real valued  $n \times n$  matrix  $C = C(p, q)$  which satisfies that for all  $u, v \in \beta_q + \mathfrak{G}_q$  we have

$$C_{u,v} = \sum_{g \in \mathfrak{G}} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X}[\rho_q(v - \beta_q + x) - \rho_q(u - \beta_q + x) + \langle g, x \rangle_\omega] \right|^{2p}$$

We need some small simplification and some further preparation before we can give the proof. Assume in the following that  $u, v \in \beta_q + \mathfrak{G}_q$ . Consider the term  $\langle g, x \rangle_\omega$  in the above equation, where  $g \in \mathfrak{G}$  and  $x \in \mathfrak{G}_q$ . Define a set  $K = \{g \in \mathfrak{G} \mid \langle g, x \rangle_\omega = 0 \text{ for all } x \in \mathfrak{G}_q\}$  which clearly is a subgroup of  $\mathfrak{G}$  and let  $\mathfrak{G}' = \mathfrak{G}/K$  be the factor group of  $\mathfrak{G}$  modulo  $K$ . Let  $f : \mathfrak{G} \rightarrow \mathfrak{G}'$  be the canonical homomorphism defined by  $g \mapsto g + K$ , which thus has kernel  $\ker f = K$ . Then the following holds

*Claim 1.* For all  $g' \in \mathfrak{G}'$  and all  $a, b \in f^{-1}(g')$  we have

$$\langle a, x \rangle_\omega = \langle b, x \rangle_\omega \text{ for all } x \in \mathfrak{G}_q.$$

And  $|\mathfrak{G}'| = |\mathfrak{G}_q|$ .

*Proof.* For the first part, we have  $a + K = b + K$ . Thus  $b = a + k$  for some  $k \in K$  which yields  $\langle b, x \rangle_\omega = \langle a, x \rangle_\omega + \langle k, x \rangle_\omega = \langle a, x \rangle_\omega$ . Let us now show that  $|\mathfrak{G}'| = |\mathfrak{G}_q|$ . Note first that the columns  $H_{*, -g} = \mathcal{X}[\langle *, g \rangle_\omega]$  for all  $g \in \mathfrak{G}_q$  form an independent set of columns. Thus there is a set  $I \subseteq \mathfrak{G}$  such that the submatrix  $H_{I, \mathfrak{G}_q}$  is non-singular. Note that by the first part of the claim, all distinct  $a, b \in I$  are contained in distinct fibers of  $f$ . That is, there are distinct  $g', g'' \in \mathfrak{G}'$  such that  $a \in f^{-1}(g')$  and  $b \in f^{-1}(g'')$ . This proves  $|\mathfrak{G}'| = |I| = |\mathfrak{G}_q|$ .  $\dashv$

By this claim, we may, for each  $g \in \mathfrak{G}'$ , fix an element  $\hat{g} \in f^{-1}(g)$  (which is always possible as  $f$  is surjective) and assume particularly that  $\hat{0} = 0$ . We obtain

$$C_{u,v} = |K| \sum_{g \in \mathfrak{G}'} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X}[\rho_q(v - \beta_q + x) - \rho_q(u - \beta_q + x) + \langle \hat{g}, x \rangle_\omega] \right|^{2p}$$

Define now  $C' = C'(p, q) = |K|^{-1} \cdot C$ . We have  $\text{EVAL}^{\text{pin}}(C') \equiv \text{EVAL}^{\text{pin}}(C)$  and for  $u, v \in \beta_q + \mathfrak{G}_q$ ,

$$C'_{uv} = \sum_{g \in \mathfrak{G}'} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X}[\rho_q(v - \beta_q + x) - \rho_q(u - \beta_q + x) + \langle \hat{g}, x \rangle_\omega] \right|^{2p} \quad (68)$$

so we may found our further considerations on  $C'$  which makes our reasoning a bit more convenient.

*Claim 2.* For all  $g \in \mathfrak{G}'$  we have the following:

- (1) If  $g = 0$  then  $\sum_{x \in \mathfrak{G}_q} \mathcal{X}[\langle \hat{g}, x \rangle_\omega] = |\mathfrak{G}_q|$ .
- (2) If  $g \neq 0$  then  $\sum_{x \in \mathfrak{G}_q} \mathcal{X}[\langle \hat{g}, x \rangle_\omega] = 0$ .

In particular, the mappings  $\{\chi_g : \mathfrak{G}_q \rightarrow \mathbb{U}_\omega \mid \chi_g := \mathcal{X}[\langle \hat{g}, * \rangle_\omega], g \in \mathfrak{G}'\}$  form a basis of the  $|\mathfrak{G}_q|$  dimensional vector space  $L^2(\mathfrak{G}_q)$  of functions  $f : \mathfrak{G}_q \rightarrow \mathbb{C}$ .

*Proof.* The statement (1) is clear from the definition of  $K$ . For statement (2) recall that  $\mathfrak{G}_q$  has a decomposition into cyclic groups  $\mathfrak{C}_1 \oplus \dots \oplus \mathfrak{C}_z$  and each  $x \in \mathfrak{G}_q$  has a representation  $x = \sum_{i=1}^z \lambda_i h_i$  with each  $h_i$  being a generator of  $\mathfrak{C}_i$  and each  $\lambda_i \in \mathbb{Z}_{\text{ord}(h_i)}$ . Thus

$$\begin{aligned} \sum_{x \in \mathfrak{G}_q} \mathcal{X}[\langle \hat{g}, x \rangle_\omega] &= \sum_{\lambda_1 \in \mathbb{Z}_{\text{ord}(h_1)}} \dots \sum_{\lambda_z \in \mathbb{Z}_{\text{ord}(h_z)}} \mathcal{X} \left[ \langle \hat{g}, \sum_{i=1}^z \lambda_i h_i \rangle_\omega \right] \\ &= \sum_{\lambda_1 \in \mathbb{Z}_{\text{ord}(h_1)}} \dots \sum_{\lambda_z \in \mathbb{Z}_{\text{ord}(h_z)}} \prod_{i=1}^z \mathcal{X}[\langle \hat{g}, h_i \rangle_\omega]^{\lambda_i} \\ &= \prod_{i=1}^z \sum_{\lambda_i \in \mathbb{Z}_{\text{ord}(h_i)}} \mathcal{X}[\langle \hat{g}, h_i \rangle_\omega]^{\lambda_i} \end{aligned}$$

By  $g \neq 0$  we know that there is an  $x \in \mathfrak{G}_q$  such that  $\langle \hat{g}, x \rangle_\omega \neq 0$ . Hence by  $x = \sum_{i=1}^z \lambda_i h_i$  there is at least one  $h_i$  such that  $\langle \hat{g}, h_i \rangle_\omega \neq 0$ . Let  $N$  be a multiple of the order of  $h_i$ . By the homomorphism property of the  $\langle *, * \rangle_\omega$  operator we have

$$\mathcal{X} [\langle \hat{g}, h_i \rangle_\omega]^N = \mathcal{X} [N \langle \hat{g}, h_i \rangle_\omega] = \mathcal{X} [\langle \hat{g}, N h_i \rangle_\omega] = \mathcal{X} [\langle \hat{g}, 0 \rangle_\omega] = 1$$

That is  $\mathcal{X} [\langle \hat{g}, h_i \rangle_\omega]$  is an  $\text{ord}(h_i)$ -th root of unity and therefore we have

$$\sum_{\lambda_i \in \mathbb{Z}_{\text{ord}(h_i)}} \mathcal{X} [\langle \hat{g}, h_i \rangle_\omega]^{\lambda_i} = 0.$$

This finishes the first part of the claim. For the second part note that we have, for  $g \neq h \in \mathfrak{G}'$ ,

$$\langle \chi_g, \chi_h \rangle = \sum_{x \in \mathfrak{G}_q} \chi_g(x) \cdot \overline{\chi_h(x)} = \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\langle \hat{g}, x \rangle_\omega - \langle \hat{h}, x \rangle_\omega] = \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\langle \hat{g} - \hat{h}, x \rangle_\omega].$$

By the first part of the claim, this value is zero iff  $\hat{g} - \hat{h} \in K$  which implies  $g = h$  by the definition of the elements  $\hat{g}$ . Therefore all distinct  $\chi_g, \chi_h$  are pairwise orthogonal. The fact that they form a basis of  $L^2(\mathfrak{G}_q)$  now follows from  $|\mathfrak{G}'| = |\mathfrak{G}_q|$  as given by Claim 1.  $\dashv$

*Claim 3.* If  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is not  $\#P$ -hard then the following is true. For all  $a \in \mathfrak{G}_q$  there is exactly one  $g \in \mathfrak{G}'$  such that

$$|\mathfrak{G}_q| = \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) + \langle \hat{g}, x \rangle_\omega] \right|$$

and for all other  $g' \in \mathfrak{G}'$  we have

$$0 = \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) + \langle \hat{g}', x \rangle_\omega] \right|$$

*Proof.* As  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  not being  $\#P$ -hard implies the same for  $\text{EVAL}^{\text{pin}}(C')$  we can, for all choices of  $p \in \mathbb{N}$ , derive the following by Lemma 4.23:

For all  $p \in \mathbb{N}$ , the matrix  $C' = C'(p, q)$  does not contain a block of rank at least  $\geq 2$ .

This is particularly true for all submatrices of  $C'$  induced by indices from the coset  $\beta_q + \mathfrak{G}_q$ . Note that equation (68), Claim 2 and  $\hat{0} = 0$ , entail that for all  $u \in \beta_q + \mathfrak{G}_q$

$$C'_{u,u} = \sum_{g \in \mathfrak{G}'} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\langle \hat{g}, x \rangle_\omega] \right|^{2p} = \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\langle \hat{0}, x \rangle_\omega] \right|^{2p} = |\mathfrak{G}_q|^{2p}.$$

Consider a  $2 \times 2$  submatrix of  $C'$  induced by  $u = \beta_q + 0$  and some  $v = \beta_q + a \in \mathfrak{G}_q$ ,

$$\begin{pmatrix} C'_{u,u} & C'_{u,v} \\ C'_{v,u} & C'_{v,v} \end{pmatrix} = \begin{pmatrix} |\mathfrak{G}_q|^{2p} & C'_{u,v} \\ C'_{u,v} & |\mathfrak{G}_q|^{2p} \end{pmatrix}.$$

As this submatrix is either not part of a single block, or it is of rank at most 1 we see that

$$\text{For all } p \in \mathbb{N} \text{ either } C'_{u,v} = 0 \text{ or } (C'_{u,v})^2 = |\mathfrak{G}_q|^{4p}. \quad (69)$$

By the choice of  $u, v$  we have

$$C'_{u,v} = \sum_{g \in \mathfrak{G}'} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) + \langle \hat{g}, x \rangle_\omega] \right|^{2p}$$

and note that the inner term  $\left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) + \langle \hat{g}, x \rangle_\omega] \right|$  is always at most  $|\mathfrak{G}_q|$ . For all  $0 \leq i \leq |\mathfrak{G}_q|$  define

$$c_{a,i} = \left| \left\{ g \in \mathfrak{G}' : \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) + \langle \hat{g}, x \rangle_\omega] \right| = i \right\} \right|.$$

This enables us to rewrite the expression for  $C'_{u,v}$  by

$$C'_{u,v} = \sum_{\nu=0}^{|\mathfrak{G}_q|} c_{a,\nu} (\nu^2)^p.$$

And  $C'_{u,u} = C'_{v,v} = |\mathfrak{G}_q|^{2p}$ . Assume first that  $C'_{u,v} = 0$  holds for infinitely many  $p$ . Then Lemma 4.4 implies that  $c_{a,0} = |\mathfrak{G}'|$  and  $c_{a,1} = \dots = c_{a,|\mathfrak{G}_q|} = 0$ . However this would mean that the mapping  $f : \mathfrak{G}_q \rightarrow \mathbb{U}$  defined by

$$f(x) := \mathcal{X} [\rho_q(a+x) - \rho_q(x)]$$

is orthogonal to all  $\chi_g$  for  $g \in \mathfrak{G}'$  in contradiction to these being a basis of  $L^2(\mathfrak{G}_q)$  — as we have seen in Claim 2. Therefore, there are infinitely many  $p$  such that  $(C'_{u,v})^2 = |\mathfrak{G}_q|^{4p}$ . That is, there are infinitely many  $p$  such that

$$|\mathfrak{G}_q|^{2p} = \sum_{\nu=0}^{|\mathfrak{G}_q|} c_{a,\nu} (\nu^2)^p$$

which by Lemma 4.4 implies that  $c_{a,0} = |\mathfrak{G}'| - 1$  and  $c_{a,1} = \dots = c_{a,|\mathfrak{G}_q|-1} = 0$  and  $c_{a,|\mathfrak{G}_q|} = 1$ . This finishes the proof.  $\dashv$

Assume from now on that  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is not  $\#P$ -hard. Then the uniqueness statement of Claim 3, implies that there is a mapping  $\gamma_q : \mathfrak{G}_q \rightarrow \mathfrak{G}$  such that for all  $a \in \mathfrak{G}_q$  we have

$$|\mathfrak{G}_q| = \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) - \langle \gamma_q(a), x \rangle_\omega] \right|$$

Further, by

$$\begin{aligned} \left| \sum_{x \in \mathfrak{G}_q} \mathcal{X} [\rho_q(a+x) - \rho_q(x) - \langle \gamma_q(a), x \rangle_\omega] \right| &\leq \\ \sum_{x \in \mathfrak{G}_q} |\mathcal{X} [\rho_q(a+x) - \rho_q(x) - \langle \gamma_q(a), x \rangle_\omega]| &= |\mathfrak{G}_q| \end{aligned}$$



we see that equality can be achieved only, if there is a constant  $\alpha_a \in \Omega$  such that for all  $x \in \mathfrak{G}_q$  we have

$$\rho_q(a+x) - \rho_q(x) - \langle \gamma_q(a), x \rangle_\omega = \alpha_a.$$

With  $x = 0$  and  $\rho_q(0) = 0$  we see that  $\alpha_a = \rho_c(a)$ . This finishes the proof.  $\square$

## 6.4 The Proof of the Non-Bipartite Case Lemma 6.1

Let  $H$  be an  $\omega$ -algebraic  $n \times n$  matrix and  $\mathbf{D}$  a family of diagonal matrices defining an **(H-STD)**-problem. Lemma 6.3 implies that  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is  $\#P$ -hard unless the group condition **(GC)** is satisfied.

Assume therefore that **(GC)** is satisfied and recall the definitions of the Representability Conditions **(R1)**–**(R5)** on page 12. We know that  $H$  and  $\mathbf{D}$  satisfy **(R1)** and **(R2)**. By Lemma 6.4 the problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is  $\#P$ -hard unless the conditions **(R3)** and **(R4)** are satisfied. By Lemma 6.5 we may further assume w.l.o.g. that **(R5)** is satisfied. Therefore the proof follows as Lemma 6.6 proves  $\#P$ -hardness of  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  unless the Affinity Condition **(AF)** holds.

## 7 Polynomial Time Computable Partition Functions

In this section we will prove Theorem 3.8. The following two lemmas yield the proof.

**Lemma 7.1.** *Let  $H$  be an  $\omega$ -algebraic  $n \times n$  matrix and  $\mathbf{D}$  a family of diagonal matrices defining an **(H-STD)**-problem which has a representation as given in conditions **(R1)** through **(R5)**. Assume further that the Affinity Condition **(AF)** is satisfied. Then the problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is polynomial time computable.*

**Lemma 7.2.** *Let  $A$  be an  $\omega$ -algebraic and  $\mathbf{D}$  a family of diagonal matrices defining a **(B-H-STD)**-problem which has a representation as given in conditions **(B-R1)** through **(B-R5)**. Assume further that the Affinity Condition **(B-AF)** is satisfied. Then the problem  $\text{EVAL}^{\text{pin}}(A, \mathbf{D})$  is polynomial time computable.*

As in the previous sections, we will give the proof only of Lemma 7.1. The proof of Lemma 7.2 is omitted due to its similarity to the former. For completeness, we refer to [Thu09] for a proof.

The proof of Lemma 7.1 relies on a reduction of the given partition function to functions  $Z_q(f)$  closely related to degree 2 polynomials  $f$  over the ring  $\mathbb{Z}_q$  ( $q$  being a prime power). In the first part of this section we will introduce these functions and show how they can be computed in polynomial time. Afterwards, we will show how to reduce the computational problems satisfying the preconditions of the Lemma to these problems. This will prove both results.

### 7.1 A Polynomial Time Computable Problem

Let  $q$  be a prime power and  $f \in \mathbb{Z}_q[X_1, \dots, X_n]$  a polynomial. Define  $\zeta_q = \exp(2\pi i \cdot q^{-1})$  – we fix this definition for the rest of this section. Define the function

$$Z_q(f) = \sum_{X_1, \dots, X_n \in \mathbb{Z}_q} \zeta_q^{f(X_1, \dots, X_n)}.$$

We say that  $f$  is of *degree 2*, if there are constants  $c_{ij}, c_i \in \mathbb{Z}_q$  such that

$$f(X_1, \dots, X_n) = \sum_{i \leq j} c_{ij} X_i X_j + \sum_{i=1}^n c_i X_i + c_0. \quad (70)$$

Let  $\text{EVAL}(q)$  denote the problem of computing  $Z_q(f)$  given a degree 2 polynomial  $f \in \mathbb{Z}_q[X_1, \dots, X_n]$ . Since it has been shown in [CCL09] that this problem is polynomial time computable, it will be central in the proof of polynomial time computability of partition functions.

**Theorem 7.3 (Theorem 12.1 in [CCL09]).** *Let  $q$  be a prime power. The problem  $\text{EVAL}(q)$  is polynomial time computable.*

## 7.2 Computing Partition Functions — The Non-Bipartite Case

We will now prove Lemma 7.1. Recall that we are given an  $\omega$ -algebraic  $n \times n$  matrix  $H$  and a family  $\mathbf{D}$  of diagonal matrices defining an **(H-STD)**-problem which has a representation as given in conditions **(R1)** through **(R5)** and the Affinity Condition **(AF)** is satisfied. We shall show that the problem  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  is polynomial time computable.

The proof relies on the reduction of  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  to the problems  $\text{EVAL}(q)$  which we have introduced in the preceding section. To make our partition functions at hand more amenable for this reduction, we will first analyze the structure of the vertex weights represented by the family  $\mathbf{D}$  a bit more.

### 7.2.1 The Structure of the Mappings $\rho_c$

Recall the mappings  $\rho_c$  as given in condition **(R4)** and assume further that they satisfy condition **(R5)** and **(AF)**. In this section we will derive an important property of these functions. Before we state it, a word of preparation is in order. Recall that the image of all mappings  $\rho_c$  lies in the Abelian group  $\Omega$  defined in condition **(R1)**. We will work with binomial coefficients which we define by  $\binom{\lambda}{2} := \frac{\lambda(\lambda-1)}{2}$  for all  $\lambda \in \mathbb{Z}$ . Observe in particular that  $\binom{\lambda}{2}$  is defined also for negative values and for each  $g \in \Omega$  the expression  $\binom{\lambda}{2} \cdot g$  is well-defined.

**Lemma 7.4.** *For every  $c \in \mathbb{Z}_\omega$  the mapping  $\rho_c$  satisfies the following. Let  $\lambda_1, \dots, \lambda_z \in \mathbb{Z}$  and  $h_1, \dots, h_z \in \mathfrak{G}_c$  then*

$$\rho_c \left( \sum_{i=1}^z \lambda_i h_i \right) = \sum_{i=1}^z \lambda_i \rho_c(h_i) + \binom{\lambda_i}{2} \langle \gamma_c(h_i), h_i \rangle_\omega + \sum_{j < i} \lambda_i \lambda_j \langle \gamma_c(h_i), h_j \rangle_\omega$$

*Furthermore, for all  $g \in \mathfrak{G}_c$  the following holds. If  $\text{ord}(g)$  is odd, then the order of  $\rho_c(g)$  divides  $\text{ord}(g)$ . If  $\text{ord}(g)$  is even, then the order of  $\rho_c(g)$  divides  $2 \cdot \text{ord}(g)$ .*

Recall the Affinity Condition **(AF)**: For all  $c \in \mathbb{Z}_\omega$  there is a  $\gamma_c : \mathfrak{G}_c \rightarrow \mathfrak{G}$  such that

$$\rho_c(y + x) - \rho_c(x) - \rho_c(y) = \langle \gamma_c(y), x \rangle_\omega \text{ for all } x, y \in \mathfrak{G}_c. \quad (71)$$

**Lemma 7.5.** *The following holds for all  $c \in \mathbb{Z}_\omega$  and  $y, y', x \in \mathfrak{G}_c$ .*

$$\langle \gamma_c(y + y'), x \rangle_\omega = \langle \gamma_c(y), x \rangle_\omega + \langle \gamma_c(y'), x \rangle_\omega \quad \text{and} \quad \langle \gamma_c(x), y \rangle_\omega = \langle \gamma_c(y), x \rangle_\omega.$$

*Proof.* By commutativity of the addition  $x + y$  equation (71) yields

$$\langle \gamma_c(y), x \rangle_\omega = \rho_c(y + x) - \rho_c(x) - \rho_c(y) = \langle \gamma_c(x), y \rangle_\omega \quad (72)$$

By the bilinearity of  $\langle *, * \rangle$  and equation (72) we have, for all  $y, y' \in \mathfrak{G}_c$ ,  $\langle \gamma_c(y + y'), x \rangle_\omega = \langle \gamma_c(x), y + y' \rangle_\omega = \langle \gamma_c(x), y \rangle_\omega + \langle \gamma_c(x), y' \rangle_\omega$ . A second application of (72) on the right hand side of this yields  $\langle \gamma_c(y + y'), x \rangle_\omega = \langle \gamma_c(y), x \rangle_\omega + \langle \gamma_c(y'), x \rangle_\omega$ .  $\square$

*Proof (of Lemma 7.4).* We will first prove that, for all  $h_1, \dots, h_z \in \mathfrak{G}_c$ ,

$$\rho_c \left( \sum_{i=1}^z h_i \right) = \sum_{i=1}^z \rho_c(h_i) + \sum_{j < i} \langle \gamma_c(h_i), h_j \rangle_\omega. \quad (73)$$

The proof is a straightforward induction on  $z$ . The case  $z = 1$  is trivially true. For  $z > 1$ , recall that by equation (71)

$$\rho_c(y + x) = \rho_c(y) + \rho_c(x) + \langle \gamma_c(x), y \rangle_\omega \text{ for all } x, y \in \mathfrak{G}_c.$$

This yields

$$\begin{aligned} \rho_c \left( \sum_{i=1}^z h_i \right) &= \rho_c \left( \sum_{i=1}^{z-1} h_i \right) + \rho_c(h_z) + \langle \gamma_c(h_z), \left( \sum_{i=1}^{z-1} h_i \right) \rangle_\omega \\ &= \sum_{i=1}^{z-1} \rho_c(h_i) + \sum_{j < i} \langle \gamma_c(h_i), h_j \rangle_\omega + \left( \rho_c(h_z) + \sum_{j=1}^{z-1} \langle \gamma_c(h_z), h_j \rangle_\omega \right). \end{aligned}$$

Here, we used the induction hypothesis for  $\rho_c \left( \sum_{i=1}^{z-1} h_i \right)$  to obtain the second equality. This proves (73). We claim that the following is true.

$$\text{For all } \lambda \in \mathbb{Z} \text{ and } h \in \mathfrak{G}_c, \text{ we have } \rho_c(\lambda h) = \lambda \rho_c(h) + \binom{\lambda}{2} \langle \gamma_c(h), h \rangle_\omega. \quad (74)$$

Before we prove this, let us see how it helps proving the Lemma. By equation (73) we have

$$\rho_c \left( \sum_{i=1}^z \lambda_i h_i \right) = \sum_{i=1}^z \rho_c(\lambda_i h_i) + \sum_{j < i} \lambda_i \lambda_j \langle \gamma_c(h_i), h_j \rangle_\omega.$$

And substituting  $\rho_c(\lambda_i h_i)$ , for all  $i \in [z]$ , with the expression given by equation (74) yields

$$\rho_c \left( \sum_{i=1}^z \lambda_i h_i \right) = \sum_{i=1}^z \lambda_i \rho_c(h_i) + \binom{\lambda_i}{2} \langle \gamma_c(h_i), h_i \rangle_\omega + \sum_{j < i} \lambda_i \lambda_j \langle \gamma_c(h_i), h_j \rangle_\omega$$

just as in the statement of the lemma.

**The proof of equation (74).** For  $\lambda = 0$  this is trivial and for  $\lambda > 0$  recall equation (73). We have

$$\rho_c(\lambda h) = \rho_c\left(\sum_{i=1}^{\lambda} h\right) = \sum_{i=1}^{\lambda} \rho_c(h) + \binom{\lambda}{2} \langle \gamma_c(h), h \rangle_{\omega}. \quad (75)$$

This proves equation (74) for  $\lambda \geq 0$ . It remains to prove the case  $\lambda < 0$ . Before we do this we need to prove the second statement of the Lemma, namely

*Claim 1.* Let  $g \in \mathfrak{G}_c$ . If  $\text{ord}(g)$  is odd, then the order of  $\rho_c(g)$  divides the order of  $g$ . If  $\text{ord}(g)$  is even, then the order of  $\rho_c(g)$  divides  $2 \cdot \text{ord}(g)$ .

*Proof.* Let  $N \geq 0$  be the order of  $g$ . That is,  $N \cdot g = 0$  and equation (75) implies

$$0 = \rho_c(0) = \rho_c(N \cdot g) = N\rho_c(g) + \binom{N}{2} \langle \gamma_c(g), g \rangle_{\omega}.$$

If  $N$  is odd then it divides  $\binom{N}{2}$  and therefore  $\binom{N}{2}g = 0$ . Hence  $\binom{N}{2} \langle \gamma_c(g), g \rangle_{\omega} = \langle \gamma_c(g), \binom{N}{2}g \rangle_{\omega} = \langle \gamma_c(g), 0 \rangle_{\omega} = 0$  and the above equation thus implies  $0 = N\rho_c(g)$ . If  $N$  is even then the same argument using  $2N$  yields the proof.  $\square$

Let us now prove equation (74) for  $\lambda < 0$ . Define  $N$  as the smallest multiple of  $2 \cdot \text{ord}(h)$  such that  $N + \lambda > 0$ , then  $\lambda h = (N + \lambda)h$  and  $\rho_c(\lambda h) = \rho_c((N + \lambda)h)$ . We may thus apply the part of equation (74) which has been proved already and obtain

$$\begin{aligned} \rho_c((N + \lambda)h) &= (N + \lambda)\rho_c(h) + \binom{N + \lambda}{2} \langle \gamma_c(h), h \rangle_{\omega} \\ &= \lambda\rho_c(h) + \binom{\lambda}{2} \langle \gamma_c(h), h \rangle_{\omega}. \end{aligned}$$

The second equality follows from Claim 1.  $\square$

From Lemma 7.4 we can derive a rather technical result which will become necessary in the proof of Lemma 7.1.

**Lemma 7.6.** *Let  $g \in \mathfrak{G}_c$  be an element of order  $q = 2^k$ . The order of the element  $2 \cdot \rho_c(g) + \langle \gamma_c(g), g \rangle_{\omega}$  in  $\mathbb{Z}_{\omega}$  is at most  $q/2$ .*

*Proof.* By Lemma 7.4 we have

$$0 = \rho_c(0) = \rho_c(q \cdot g) = q\rho_c(g) + \binom{q}{2} \langle \gamma_c(g), g \rangle_{\omega}. \quad (76)$$

and the order of  $\rho_c(g)$  divides  $2q$ . Note that the order of  $\langle \gamma_c(g), g \rangle_{\omega}$  divides  $q$  by  $q \langle \gamma_c(g), g \rangle_{\omega} = \langle \gamma_c(g), q \cdot g \rangle_{\omega} = \langle \gamma_c(g), 0 \rangle_{\omega} = 0$ .

Assume first that the order of  $\langle \gamma_c(g), g \rangle_{\omega}$  equals  $q$ . Then the element  $2 \cdot \rho_c(g) + \langle \gamma_c(g), g \rangle_{\omega}$  has order at most  $q/2$  only if the order of  $2\rho_c(g)$  is  $q$ , as well. Assume therefore, for contradiction, that the order of  $2\rho_c(g)$  divides  $q/2$ . Equation (76) implies

$$0 = \binom{q}{2} \langle \gamma_c(g), g \rangle_{\omega}.$$

As  $q - 1$  is odd,  $q$  does not divide  $\binom{q}{2}$  — a contradiction.

Assume now that the order of  $\langle \gamma_c(g), g \rangle_{\omega}$  is strictly smaller than  $q$ , that is  $q/2 \cdot \langle \gamma_c(g), g \rangle_{\omega} = 0$ . As  $q/2$  divides  $\binom{q}{2}$  equation (76) implies that  $0 = q\rho_c(g)$ . This finishes the proof.  $\square$

### 7.2.2 The Final Reduction

We will now prove Lemma 7.1. We start with some preliminaries. Consider  $\mathbb{Z}_q$ -polynomial  $f$  of degree 2 as in equation (70). With each variable  $X_i$  we associate an order  $\text{ord}(X_i)$  which divides  $q$ . A degree 2 monomial  $c_{ij}X_iX_j$  for  $i \neq j$  is called *consistent* if the values  $c_{ij} \cdot \text{ord}(X_i)$  and  $c_{ij} \cdot \text{ord}(X_j)$  are divisible by  $q$ . Similarly, a monomial  $c_iX_i$  is consistent if  $q$  divides  $c_i \cdot \text{ord}(X_i)$ . Finally, a *square monomial*  $c_{ii}X_i^2$  is consistent if  $2 \cdot c_{ii} \cdot \text{ord}(X_i)$  is divisible by  $q$ .

**Lemma 7.7.** *Let  $q$  be a prime power. The following problem can be reduced to  $\text{EVAL}(q)$  in polynomial time. The input consists of a degree 2 polynomial  $f \in \mathbb{Z}_q[X_1, \dots, X_n]$  of the form given by equation (70). Each variable  $X_i$  has an order  $\text{ord}(X_i)$  which divides  $q$  and all non-constant monomials are consistent. The task is to compute the value*

$$\sum_{X_1 \in \mathbb{Z}_{\text{ord}(X_1)}} \cdots \sum_{X_n \in \mathbb{Z}_{\text{ord}(X_n)}} \zeta_q^{f(X_1, \dots, X_n)}.$$

*Proof.* To perform the reduction of the problem at hand to  $\text{EVAL}(q)$  we will need to show how to “lift” the order of each variable  $X_i$  to  $q$ . Assume w.l.o.g. that the order  $x_i := \text{ord}(X_i)$  of each variable is greater than 1. Fix some variable  $X_\nu$ . We will have a look at the situation after the order of  $X_\nu$  has been lifted. For all  $i \in [n]$  define  $q_i = q \cdot x_i^{-1}$ . We have

$$\sum_{\forall i \neq \nu: X_i \in \mathbb{Z}_{x_i}} \sum_{X_\nu \in \mathbb{Z}_q} \zeta_q^{f(X_1, \dots, X_\nu, \dots, X_n)} = \sum_{\forall i \neq \nu: X_i \in \mathbb{Z}_{x_i}} \sum_{X_\nu \in \mathbb{Z}_{x_\nu}} \sum_{j=0}^{q_\nu-1} \zeta_q^{f(X_1, \dots, X_\nu+j \cdot x_\nu, \dots, X_n)}. \quad (77)$$

Let  $\ell(X_1, \dots, \hat{X}_\nu, \dots, X_n) = \sum_{i < \nu} c_{i\nu}X_i + \sum_{\nu < i} c_{\nu i}X_i$  and fix the degree 2 polynomial  $h$  which captures the part of  $f$  not involving  $X_\nu$ . We have

$$f(X_1, \dots, X_n) = c_{\nu\nu}X_\nu^2 + X_\nu \cdot \ell(X_1, \dots, \hat{X}_\nu, \dots, X_n) + h(X_1, \dots, \hat{X}_\nu, \dots, X_n).$$

Further

$$\begin{aligned} f(X_1, \dots, X_\nu + j \cdot x_\nu, \dots, X_n) &= c_{\nu\nu}(X_\nu + j \cdot x_\nu)^2 + (X_\nu + j \cdot x_\nu) \cdot \ell + h \\ &= c_{\nu\nu}X_\nu^2 + 2c_{\nu\nu}x_\nu \cdot jX_\nu + c_{\nu\nu}x_\nu^2 \cdot j^2 + X_\nu\ell + jx_\nu\ell + h \end{aligned}$$

By the consistency of the monomials  $c_iX_i$  and that of  $c_{ij}X_iX_j$  for all  $i \neq j$  we see that all coefficients of  $x_\nu\ell$  are divisible by  $q$ . This is also true for  $2c_{\nu\nu}x_\nu$ . To see this for  $c_{\nu\nu}x_\nu^2$  note first that if  $q$  is a power of 2 then  $c_{\nu\nu}x_\nu^2$  is divisible by  $2c_{\nu\nu}x_\nu$  as 2 divides  $x_\nu$ . Otherwise the condition that  $2c_{\nu\nu}x_\nu$  be divisible by  $q$  is equivalent to  $c_{\nu\nu}x_\nu$  being divisible by  $q$ . Therefore, for all  $j \in \{0, \dots, q_\nu - 1\}$  we have  $f(X_1, \dots, X_\nu + j \cdot x_\nu, \dots, X_n) \equiv c_{\nu\nu}X_\nu^2 + X_\nu\ell + h \pmod{q}$ . Using equation (77), we see that

$$\sum_{\forall i \neq \nu: X_i \in \mathbb{Z}_{x_i}} \sum_{X_\nu \in \mathbb{Z}_q} \zeta_q^{f(X_1, \dots, X_n)} = q_\nu \cdot \sum_{X_1 \in \mathbb{Z}_{x_1}} \cdots \sum_{X_n \in \mathbb{Z}_{x_n}} \zeta_q^{f(X_1, \dots, X_n)}.$$

As this holds independently for all  $\nu \in [n]$ , it follows that

$$Z_q(f(X_1, \dots, X_n)) = \left( \prod_{i=1}^n q_i \right) \sum_{X_1 \in \mathbb{Z}_{x_1}} \cdots \sum_{X_n \in \mathbb{Z}_{x_n}} \zeta_q^{f(X_1, \dots, X_n)}.$$

This finishes the proof.  $\square$

### 7.2.3 The proof of Lemma 7.1

*Proof (of Lemma 7.1).* Let now  $\text{EVAL}^{\text{pin}}(H, \mathbf{D})$  be an **(H-STD)** problem which meets all conditions **(R1)**–**(R4)** and **(AF)**. Let  $G = (V, E)$  be a digraph and  $\phi$  a pinning. With  $V' = V \setminus \text{def}(\phi)$  we have

$$Z_{H, \mathbf{D}}(\phi, G) = \sum_{\phi \subseteq \sigma: V \rightarrow \mathfrak{G}} \prod_{uv \in E} H_{\sigma(u), -\sigma(v)} \prod_{v \in V'} D_{\sigma(v), \sigma(v)}^{\llbracket \partial(v) \rrbracket} \quad (78)$$

We shall prove that  $Z_{H, \mathbf{D}}(\phi, G)$  can be computed in polynomial time. To do this, we will present a polynomial time reduction to the problems  $\text{EVAL}(q)$ . Most of this proof will be devoted to rewriting the expression of this partition function into a form which resembles the expression  $Z_q(f)$  used in  $\text{EVAL}(q)$ .

Recall the representation of  $H$  and  $\mathbf{D}$  as given in conditions **(R1)**–**(R5)** on page 12. Note that a configuration  $\sigma$  which maps some vertex  $v \in V'$  to  $\sigma(v) \notin \Lambda_{\llbracket \partial(v) \rrbracket}$  does not contribute to this partition function. Assume therefore that  $\sigma(v) \in \Lambda_{\llbracket \partial(v) \rrbracket}$  is satisfied for all  $v \in V$ . Slightly abusing notation we will denote  $\Lambda_{\llbracket \partial(v) \rrbracket}$  by  $\Lambda_v = \beta_v + \mathfrak{G}_v$ . We introduce, for each  $v \in V$  a variable  $\sigma_v \in \mathfrak{G}_v$ . For all  $v \in \text{def}(\phi)$  we assume that the value of  $\sigma_v$  is fixed to  $\sigma_v = \phi(v)$ . Application of the representation **(R1)**–**(R5)** thus yields

$$\begin{aligned} Z_{H, \mathbf{D}}(\phi, G) &= \sum_{v \in V'} \sum_{\sigma_v \in \mathfrak{G}_v} \prod_{uv \in E} H_{\beta_u + \sigma_u, -(\beta_v + \sigma_v)} \prod_{v \in V'} D_{\beta_v + \sigma_v, \beta_v + \sigma_v}^{\llbracket \partial(v) \rrbracket} \\ &= \sum_{v \in V'} \sum_{\sigma_v \in \mathfrak{G}_v} \mathcal{X} \left[ \sum_{uv \in E} \langle \beta_u + \sigma_u, \beta_v + \sigma_v \rangle_{\omega} + \sum_{v \in V'} \rho_{\llbracket \partial(v) \rrbracket}(\sigma_v) \right] \end{aligned}$$

Let us rewrite the expression  $\sum_{uv \in E} \langle \beta_u + \sigma_u, \beta_v + \sigma_v \rangle_{\omega}$  a little bit. Denote by  $\mu_{uv}$  for all  $u, v \in V$  the multiplicity of the edge  $uv$  in  $E$ . Then, using the skew-bilinearity of the  $\langle *, * \rangle_{\omega}$  operator,

$$\begin{aligned} \sum_{uv \in E} \langle \beta_u + \sigma_u, \beta_v + \sigma_v \rangle_{\omega} &= \sum_{u, v \in V} \mu_{uv} \langle \beta_u + \sigma_u, \beta_v + \sigma_v \rangle_{\omega} \\ &= \sum_{u, v \in V} \mu_{uv} (\langle \beta_u, \beta_v \rangle_{\omega} + \langle \beta_u, \sigma_v \rangle_{\omega} - \langle \beta_v, \sigma_u \rangle_{\omega} + \langle \sigma_u, \sigma_v \rangle_{\omega}) \end{aligned}$$

For each  $v \in V$  define the value  $\eta_v = \sum_{u \in V} (\mu_{uv} - \mu_{vu}) \beta_u$ . Then

$$\sum_{uv \in E} \langle \beta_u + \sigma_u, \beta_v + \sigma_v \rangle_{\omega} = \sum_{u, v \in V} \mu_{uv} \langle \beta_u, \beta_v \rangle_{\omega} + \mu_{uv} \langle \sigma_u, \sigma_v \rangle_{\omega} + \sum_{v \in V} \langle \eta_v, \sigma_v \rangle_{\omega}$$

Let  $\rho_v$  denote the mapping  $\rho_{\llbracket \partial(v) \rrbracket}$  and define a value

$$c = \mathcal{X} \left[ \sum_{u, v \in V} \mu_{uv} \langle \beta_u, \beta_v \rangle_{\omega} + \sum_{v \in \text{def}(\phi)} \langle \eta_v, \sigma_v \rangle_{\omega} \right]$$

The value  $c$  is constant for all different values the  $\sigma_v$  corresponding to  $v \in V'$  may assume. We have

$$Z_{H, \mathbf{D}}(\phi, G) = \sum_{v \in V'} \sum_{\sigma_v \in \mathfrak{G}_v} \mathcal{X} \left[ \sum_{u, v \in V} \mu_{uv} \langle \beta_u, \beta_v \rangle_{\omega} + \mu_{uv} \langle \sigma_u, \sigma_v \rangle_{\omega} + \sum_{v \in V} \langle \eta_v, \sigma_v \rangle_{\omega} + \sum_{v \in V'} \rho_v(\sigma_v) \right]$$

which, by a straightforward computation yields

$$Z_{H,\mathbf{D}}(\phi, G) = c \cdot \sum_{v \in V'} \sum_{\sigma_v \in \mathfrak{G}_v} \mathcal{X} \left[ \sum_{u, v \in V} \mu_{uv} \langle \sigma_u, \sigma_v \rangle_\omega + \sum_{v \in V'} \langle \eta_v, \sigma_v \rangle_\omega + \rho_v(\sigma_v) \right] \quad (79)$$

We will proceed by further rewriting the terms of the expression

$$\sum_{u, v \in V} \mu_{uv} \langle \sigma_u, \sigma_v \rangle_\omega + \sum_{v \in V'} \langle \eta_v, \sigma_v \rangle_\omega + \rho_v(\sigma_v). \quad (80)$$

For some technical reason which will become clear later, we now decompose  $2\omega$  into prime powers. Let  $\omega_1 \cdots \omega_t = 2\omega$  be a decomposition of  $2\omega$  into powers of pairwise distinct primes. Denote by  $p_\nu$  the prime corresponding to  $\omega_\nu$  and assume w.l.o.g. that  $\omega_1$  is a power of 2 — if  $\omega$  is not divisible by 2 then we let  $\omega_1 = 2$ .

Recall once more the representation given by **(R1)**–**(R5)** on page 12. We have  $\mathfrak{G} = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_z}$  for some prime powers  $q_i$ . It will be convenient to write this decomposition of  $\mathfrak{G}$  in terms of the above prime decomposition of  $2\omega$ . Define sets  $P_\nu = \{i \in [z] \mid p_\nu \text{ divides } q_i\}$  for each  $\nu \in [t]$ . By condition **(R2)**, the order of each  $g \in \mathfrak{G}$  divides  $\omega$  implying that the  $P_1, \dots, P_t$  form a partition (with possibly empty parts) of  $[z]$ .

Therefore, we rewrite the decomposition of  $\mathfrak{G}$  by  $\mathfrak{G} = \bigoplus_{\nu=1}^t \bigoplus_{i \in P_\nu} \mathbb{Z}_{q_i}$ . Further, with each  $\mathfrak{G}_c$  being a subgroup of  $\mathfrak{G}$  we see that they also have decompositions  $\mathfrak{G}_c = \bigoplus_{\nu=1}^t \bigoplus_{i \in P_\nu} \mathbb{Z}_{q_{c,i}}$  such that w.l.o.g.  $q_{c,i}$  divides  $q_i$  for all  $c \in \mathbb{Z}_\omega$  and all  $i \in [z]$ . Let  $g_{c,i}$  be a generator of  $\mathbb{Z}_{q_{c,i}}$  for all  $c \in \mathbb{Z}_\omega$ ,  $\nu \in [t]$  and  $i \in P_\nu$ . For notational convenience, for every  $v \in V$  we denote by  $g_{v,i}$  the element  $g_{\llbracket \partial(v) \rrbracket, i}$  for all  $i \in [z]$ .

Define a vector  $\mathbf{X} = (X_{(v,i)})_{v \in V, i \in [z]}$ . Every  $\sigma_v \in \mathfrak{G}_v$  has a representation in terms of a tuple  $(X_{(v,1)}, \dots, X_{(v,z)})$  of variables each satisfying  $X_{(v,i)} \in \mathbb{Z}_{q_{v,i}}$  such that

$$\sigma_v = \sum_{i=1}^z X_{(v,i)} g_{v,i}. \quad (81)$$

Define matrices  $\Gamma$ ,  $\Delta$  and a vector  $\Lambda$ , with indices in  $V \times [z]$  such that, for all  $(u, i), (v, j) \in V \times [z]$ ,

$$\Delta_{(u,i)(v,j)} = \begin{cases} \langle \gamma_v(g_{v,i}), g_{v,j} \rangle_\omega & , \text{ if } u = v \in V' \text{ and } j < i \\ 0 & , \text{ otherwise.} \end{cases} \quad (82)$$

$$\Gamma_{(u,i)(v,j)} = \mu_{uv} \cdot \langle g_{u,i}, g_{v,j} \rangle_\omega \quad (83)$$

$$\Lambda_{(v,i)} = \begin{cases} \rho_v(g_{v,i}) + \langle \eta_v, g_{v,i} \rangle_\omega & , \text{ if } v \in V', i \in [z] \\ 0 & , \text{ otherwise.} \end{cases} \quad (84)$$

Further, define vectors  $\mathbf{B}(\mathbf{X})$  and  $\Xi$  such that for all  $(v, i) \in V \times [z]$ ,

$$\mathbf{B}(\mathbf{X})_{(v,i)} = \begin{cases} \binom{X_{(v,i)}}{2} & , \text{ if } v \in V', i \in [z] \\ 0 & , \text{ otherwise.} \end{cases} \quad (85)$$

$$\Xi_{(v,i)} = \begin{cases} \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega & , \text{ if } v \in V', i \in [z] \\ 0 & , \text{ otherwise.} \end{cases} \quad (86)$$

We can now rewrite the terms of equation (80). Applying equation (81) and the definition of  $\Gamma$  in (83), we find that

$$\sum_{u,v \in V} \mu_{uv} \langle \sigma_u, \sigma_v \rangle_\omega = \sum_{u,v \in V} \sum_{i,j=1}^z X_{(u,i)} X_{(v,j)} \cdot \mu_{uv} \langle g_{u,i}, g_{v,j} \rangle_\omega = \mathbf{X} \Gamma \mathbf{X}^T.$$

Further we have, for each  $v \in V'$

$$\begin{aligned} \langle \eta_v, \sigma_v \rangle_\omega + \rho_v(\sigma_v) &= \sum_{i=1}^z X_{(v,i)} \langle \eta_v, g_{v,i} \rangle_\omega + \rho_v \left( \sum_{i=1}^z X_{(v,i)} g_{v,i} \right) \\ &= \sum_{i=1}^z X_{(v,i)} (\rho_v(g_{v,i}) + \langle \eta_v, g_{v,i} \rangle_\omega) + \binom{X_{(v,i)}}{2} \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega \\ &\quad + \sum_{j < i} X_{(v,i)} X_{(v,j)} \langle \gamma_v(g_{v,i}), g_{v,j} \rangle_\omega. \end{aligned}$$

where the second equality follows from Lemma 7.4. By the definition of  $\Delta, \Lambda, \mathbf{B}(\mathbf{X})$  and  $\Xi$  this can be rewritten into

$$\sum_{v \in V'} \langle \eta_v, \sigma_v \rangle_\omega + \rho_v(\sigma_v) = \mathbf{X} \cdot \Lambda^T + \mathbf{X} \Delta \mathbf{X}^T + \mathbf{B}(\mathbf{X}) \cdot \Xi^T$$

Define  $f(\mathbf{X}) = \mathbf{X} \Gamma \mathbf{X}^T + \mathbf{X} \cdot \Lambda^T + \mathbf{X} \Delta \mathbf{X}^T + \mathbf{B}(\mathbf{X}) \cdot \Xi^T$ . By equation (79) we therefore have

$$Z_{H,\mathbf{D}}(\phi, G) = c \cdot \sum_{\mathbf{X}} \mathcal{X}[f(\mathbf{X})] \quad (87)$$

where the sum is over all vectors  $\mathbf{X} = (X_{(v,i)})_{(v,i) \in V' \times [z]}$  such that  $X_{(v,i)} \in \mathbb{Z}_{q_{v,i}}$  for all  $(v,i) \in V' \times [z]$ . For all  $(v,i) \in \text{def}(\phi) \times [z]$  the values  $X_{(v,i)}$  are fixed so as to satisfy  $\sigma_v = \phi(v)$ . Note that this is always possible by the definition of  $\sigma_v$  in equation (81). We call any vector  $\mathbf{X}$  satisfying these conditions a *valid assignment*.

We will simplify the description of  $f$  further. Define  $\mathcal{I} = \{I_\nu \mid \nu \in [t]\}$  with  $I_\nu = \{(v,i) \mid v \in V, i \in P_\nu\}$  — That is, the sets  $I_\nu$  form a partition of  $V \times [z]$ . Recall that  $X_I$  and  $\Delta_{IJ}$  denote subvectors and submatrices of  $X$  and  $\Delta$  induced by the indices in  $I$  and  $J$ . Then

$$f(\mathbf{X}) = \sum_{I,J \in \mathcal{I}} \mathbf{X}_I \Gamma_{IJ} \mathbf{X}_J^T + \mathbf{X}_I \Delta_{IJ} \mathbf{X}_J^T + \sum_{I \in \mathcal{I}} \mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T$$

We will claim that the "cross-terms" in this expression are zero, i.e.

$$f(\mathbf{X}) = \sum_{I \in \mathcal{I}} \mathbf{X}_I \Gamma_{II} \mathbf{X}_I^T + \mathbf{X}_I \Delta_{II} \mathbf{X}_I^T + \mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T.$$

To see this, we shall prove that, for all  $I, J \in \mathcal{I}$  with  $I \neq J$  we have  $\Gamma_{IJ} = 0$  and  $\Delta_{IJ} = 0$ . We show this for  $\Delta_{IJ}$ , the result follows analogously for  $\Gamma$ . By definition (cf. equation (82)), for  $v \in V, i \in I$  and  $j \in J$  we have  $\Delta_{(v,i)(v,j)} = \langle \gamma_v(g_{v,i}), g_{v,j} \rangle_\omega$ . By the properties of  $\gamma_v$  (cf. Lemma 7.5) and the bilinearity of  $\langle *, * \rangle_\omega$  we have  $N \langle \gamma_v(g_{v,i}), g_{v,j} \rangle_\omega = \langle \gamma_v(N g_{v,i}), g_{v,j} \rangle_\omega = \langle \gamma_v(g_{v,i}), N g_{v,j} \rangle_\omega$ . Therefore the order of  $\Delta_{(v,i)(v,j)}$  divides both,  $\text{ord}_{\mathfrak{S}}(g_{v,i})$  and  $\text{ord}_{\mathfrak{S}}(g_{v,j})$ . By our choice of  $I$  and  $J$  these orders are co-prime and the claim follows. Define

$$f_\nu(\mathbf{X}_I) = \mathbf{X}_I \Gamma_{II} \mathbf{X}_I^T + \mathbf{X}_I \Delta_{II} \mathbf{X}_I^T + \mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T \text{ for every } \nu \text{ and } I = I_\nu. \quad (88)$$



Thus

$$f(\mathbf{X}) = \sum_{\nu=1}^t f_{\nu}(\mathbf{X}_{I_{\nu}})$$

*Claim 1.* The order of all entries of  $\Gamma, \Delta$  and  $\Xi$  divides  $\omega$  and the order of all entries of  $\Lambda$  divides  $2\omega$ .

*Proof.* For  $\Delta, \Gamma$  and  $\Xi$  this follows directly from their definitions in equations (82), (83) and (86). Every non-zero entry of  $\Lambda$  satisfies  $\Lambda_{(v,i)} = \rho_v(g_{v,i}) + \langle \eta_v, g_{v,i} \rangle_{\omega}$  and the claim follows from Lemma 7.4.  $\dashv$

*Claim 2.* Let  $\nu \in [t]$  and  $I = I_{\nu}$ , then all non-zero entries of the matrices  $\Gamma_{II}$ ,  $\Delta_{II}$  and the vectors  $\Lambda_I$  and  $\Xi_I$  are divisible by  $\omega_{\mu}$  for all  $\mu \neq \nu$ .

*Proof.* For  $(u, i), (v, j) \in I_{\nu}$  we have  $\Gamma_{(u,i),(v,j)} = \mu_{uv} \cdot \langle g_{u,i}, g_{v,j} \rangle_{\omega}$ . The order of this element (in  $\mathbb{Z}_{2\omega}$ ) is some divisor of  $\omega_{\nu}$  and therefore the element itself is divisible by  $2\omega \cdot (\omega_{\nu})^{-1}$ . The proofs of the other statements follow analogously.  $\dashv$

Claim 1 implies that  $f(\mathbf{X}) \in \mathbb{Z}_{2\omega}$  for all valid assignments of  $\mathbf{X}$ . Define  $\mathcal{X}_{2\omega}(x) = \exp(\frac{2\pi i x}{2\omega})$ . We see that

$$Z_{H,\mathbf{D}}(\phi, G) = c \cdot \sum_{\alpha \in \mathbb{Z}_{2\omega}} \mathcal{X}_{2\omega}[\alpha] \cdot |\{\mathbf{X} : f(\mathbf{X}) \equiv \alpha \pmod{2\omega}\}|$$

By Claim 2 we see further that  $f(\mathbf{X}) \equiv \alpha \pmod{2\omega}$  is equivalent to a system of simultaneous congruences given by  $f_{\nu}(\mathbf{X}_{I_{\nu}}) \equiv \alpha \pmod{\omega_{\nu}}$  for all  $\nu \in [t]$ . We have

$$Z_{H,\mathbf{D}}(\phi, G) = c \cdot \sum_{\alpha \in \mathbb{Z}_{2\omega}} \mathcal{X}_{2\omega}[\alpha] \prod_{\nu=1}^t |\{\mathbf{X}_{I_{\nu}} : f_{\nu}(\mathbf{X}_{I_{\nu}}) \equiv \alpha \pmod{\omega_{\nu}}\}|$$

By the Chinese Remainder Theorem each  $\alpha$  can be written uniquely as  $\alpha = \sum_{\nu=1}^t \frac{2\omega}{\omega_{\nu}} \cdot \alpha_{\nu}$  for values  $\alpha_{\nu} \in [0, \omega_{\nu} - 1]$ . Recall that by  $\zeta_q$  we denote the value  $\zeta_q = \exp(2\pi i \cdot q^{-1})$ . Then

$$\begin{aligned} Z_{H,\mathbf{D}}(\phi, G) &= c \cdot \sum_{\alpha_1 \in \mathbb{Z}_{\omega_1}} \cdots \sum_{\alpha_t \in \mathbb{Z}_{\omega_t}} \prod_{\nu=1}^t \mathcal{X}_{2\omega} \left[ \frac{2\omega}{\omega_{\nu}} \cdot \alpha_{\nu} \right] \cdot |\{\mathbf{X}_{I_{\nu}} : f_{\nu}(\mathbf{X}_{I_{\nu}}) \equiv \alpha_{\nu} \pmod{\omega_{\nu}}\}| \\ &= c \cdot \prod_{\nu=1}^t \sum_{\alpha_{\nu} \in \mathbb{Z}_{\omega_{\nu}}} \zeta_{\omega_{\nu}}^{\alpha_{\nu}} \cdot |\{\mathbf{X}_{I_{\nu}} : f_{\nu}(\mathbf{X}_{I_{\nu}}) \equiv \alpha_{\nu} \pmod{\omega_{\nu}}\}| \end{aligned}$$

The partition function  $Z_{H,\mathbf{D}}(\phi, G)$  thus simplifies to

$$Z_{H,\mathbf{D}}(\phi, G) = c \cdot \prod_{\nu=1}^t \sum_{\mathbf{X}_{I_{\nu}}} \zeta_{\omega_{\nu}}^{f_{\nu}(\mathbf{X}_{I_{\nu}})}$$

and its computation reduces to the computation of  $t$  many independent values of the form

$$\sum_{\mathbf{X}_{I_{\nu}}} \zeta_{\omega_{\nu}}^{f_{\nu}(\mathbf{X}_{I_{\nu}})}. \quad (89)$$

We shall show now, that each of these problems satisfies the preconditions of Lemma 7.7. This then implies that each problem is reducible to  $\text{EVAL}(\omega_\nu)$  and therefore polynomial time computable by Theorem 7.3.

Fix some  $\nu \in [t]$ . To show that the problem (89) satisfies the preconditions of Lemma 7.7, we have to show that the monomials in  $f_\nu$  are consistent. In particular, the square monomials have to be consistent. Recall that this means that they are of the form  $b \cdot X_{(v,i)}^2$  such that  $2 \cdot b \cdot \text{ord}(X_{(v,i)}) = 2 \cdot b \cdot q_{v,i}$  is divisible by  $q$ . By equation (88) and  $I = I_\nu$ , we have

$$f_\nu(\mathbf{X}_I) = \mathbf{X}_I \Gamma_{II} \mathbf{X}_I^T + \mathbf{X}_I \Delta_{II} \mathbf{X}_I^T + \mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T.$$

Observe that the condition  $\sigma_v = \phi(v)$  for all  $v \in \text{def}(\phi)$  turns some variables  $X_{(v,i)}$  into constants. Therefore, some degree 2 monomials turn into linear ones and others of these and some linear ones turn into constants. Therefore, to show that the consistency preconditions of Lemma 7.7 are satisfied, it suffices to do this for the original polynomial  $f_\nu$ . For the terms  $\mathbf{X}_I \Gamma_{II} \mathbf{X}_I^T + \mathbf{X}_I \Delta_{II} \mathbf{X}_I^T$  the consistency of the corresponding monomial follows from their definition. It remains to consider the monomials arising from  $\mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T$ . Recall that

$$\mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T = \sum_{(v,i) \in I} X_{(v,i)} \cdot (\rho_v(g_{v,i}) + \langle \eta_v, g_{v,i} \rangle_\omega) + \binom{X_{(v,i)}}{2} \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega \quad (90)$$

**Case A.**  $\nu \neq 1$ . We have  $\omega_\nu$  a prime power of some odd prime  $p_\nu$ . Note that 2 has a multiplicative inverse in  $\mathbb{Z}_{\omega_\nu}$  and therefore the term

$$\binom{X_{(v,i)}}{2} \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega = \frac{X_{(v,i)} (X_{(v,i)} - 1)}{2} \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega$$

in equation (90) produces consistent monomials. Further, the term  $X_{(v,i)} \cdot (\rho_v(g_{v,i}) + \langle \eta_v, g_{v,i} \rangle_\omega)$  is consistent as well. To see this, note that  $X_{(v,i)} \cdot \langle \eta_v, g_{v,i} \rangle_\omega$  is consistent by definition of  $X_{(v,i)}$  since  $\text{ord}(X_{(v,i)}) = \text{ord}(g_{v,i})$ . By Lemma 7.4 the term  $X_{(v,i)} \cdot \rho_v(g_{v,i})$  is consistent as the order of  $g_{v,i}$  is odd.

**Case B.**  $\nu = 1$ . By equation (90) we have

$$\begin{aligned} \mathbf{X}_I \cdot \Lambda_I^T + \mathbf{B}(\mathbf{X})_I \cdot \Xi_I^T &= \sum_{(v,i) \in I} X_{(v,i)} \cdot (\rho_v(g_{v,i}) + \langle \eta_v, g_{v,i} \rangle_\omega - 2^{-1} \cdot \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega) \\ &\quad + \sum_{(v,i) \in I} X_{(v,i)}^2 \cdot 2^{-1} \cdot \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega \end{aligned}$$

Note that the expression  $2^{-1} \cdot \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega$  is well-defined, as  $\langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega$  has, by definition of  $\omega_1$ , order at most  $\omega_1/2$ . This proves that for the above square terms we have

$$2 \cdot \text{ord}(X_{(v,i)}) \cdot 2^{-1} \cdot \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega = \text{ord}(X_{(v,i)}) \cdot \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega$$

is divisible by  $\omega_1$ . Further,  $X_{(v,i)} \cdot \langle \eta_v, g_{v,i} \rangle_\omega$  is consistent. And it remains to show this for  $X_{(v,i)} \cdot (\rho_v(g_{v,i}) - 2^{-1} \cdot \langle \gamma_v(g_{v,i}), g_{v,i} \rangle_\omega)$  — which follows from Lemma 7.6.  $\square$

## References

- [BDG<sup>+</sup>08] Andrei Bulatov, Martin E. Dyer, Leslie Ann Goldberg, Markus Jalsenius, and David Richerby, *The complexity of weighted boolean #csp with mixed signs*, CoRR **abs/0812.4171** (2008).
- [BG05] Andrei A. Bulatov and Martin Grohe, *The complexity of partition functions.*, Theor. Comput. Sci. **348** (2005), no. 2-3, 148–186.
- [BK09] Libor Barto and Marcin Kozik, *Constraint satisfaction problems of bounded width*, FOCS, IEEE Computer Society, 2009, pp. 595–603.
- [Bul06] Andrei A. Bulatov, *A dichotomy theorem for constraint satisfaction problems on a 3-element set*, J. ACM **53** (2006), no. 1, 66–120.
- [Bul08] ———, *The complexity of the counting constraint satisfaction problem*, ICALP (1) (Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfssdóttir, and Igor Walukiewicz, eds.), Lecture Notes in Computer Science, vol. 5125, Springer, 2008, pp. 646–661.
- [CC09] Jin-Yi Cai and Xi Chen, *A decidable dichotomy theorem on directed graph homomorphisms with non-negative weights*.
- [CCL09] Jin-yi Cai, Xi Chen, and Pinyan Lu, *Graph homomorphisms with complex values: A dichotomy theorem*, CoRR **abs/0903.4728** (2009).
- [CH96] Nadia Creignou and Miki Hermann, *Complexity of generalized satisfiability counting problems*, Inf. Comput. **125** (1996), no. 1, 1–12.
- [CLX09] Jin-yi Cai, Pinyan Lu, and Mingji Xia, *Holant problems and counting csp*, STOC (Michael Mitzenmacher, ed.), ACM, 2009, pp. 715–724.
- [Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR MR1228206 (94i:11105)
- [DG00] Martin E. Dyer and Catherine S. Greenhill, *The complexity of counting graph homomorphisms.*, Random Struct. Algorithms **17** (2000), no. 3-4, 260–289.
- [DGJ08] Martin E. Dyer, Leslie Ann Goldberg, and Mark Jerrum, *A complexity dichotomy for hypergraph partition functions*, CoRR **abs/0811.0037** (2008).
- [DGJ09] ———, *The complexity of weighted boolean csp*, SIAM J. Comput. **38** (2009), no. 5, 1970–1986.
- [DGJR09] Martin E. Dyer, Leslie Ann Goldberg, Markus Jalsenius, and David Richerby, *The complexity of approximating bounded-degree boolean #csp*, CoRR **abs/0907.2663** (2009).
- [DGP07] Martin E. Dyer, Leslie Ann Goldberg, and Mike Paterson, *On counting homomorphisms to directed acyclic graphs*, Journal of the ACM **54** (2007), no. 6.

- [dlHJ93] P. de la Harpe and V. F. R. Jones, *Graph invariants related to statistical mechanical models: examples and problems*, J. Combin. Theory Ser. B **57** (1993), no. 2, 207–227. MR MR1207488 (94c:05033)
- [DR10] Martin E. Dyer and David Richerby, *The complexity of #csp*, To appear in STOC (2010).
- [FLS07] Michael Freedman, László Lovász, and Alexander Schrijver, *Reflection positivity, rank connectivity, and homomorphism of graphs*, J. Amer. Math. Soc. **20** (2007), no. 1, 37–51 (electronic). MR MR2257396 (2007h:05153)
- [FV98] Tomás Feder and Moshe Y. Vardi, *The computational structure of monotone monadic snp and constraint satisfaction: A study through datalog and group theory*, SIAM J. Comput. **28** (1998), no. 1, 57–104.
- [GGJT09] Leslie Ann Goldberg, Martin Grohe, Mark Jerrum, and Marc Thurley, *A complexity dichotomy for partition functions with mixed signs*, STACS (Susanne Albers and Jean-Yves Marion, eds.), Dagstuhl Seminar Proceedings, vol. 09001, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2009, pp. 493–504.
- [HN90] P. Hell and J. Nešetřil, *On the complexity of  $H$ -coloring*, Journal of Combinatorial Theory, Series B **48** (1990), 92–110.
- [JS93] Mark Jerrum and Alistair Sinclair, *Polynomial-time approximation algorithms for the ising model*, SIAM J. Comput. **22** (1993), no. 5, 1087–1116.
- [JVV90] F. Jaeger, D. L. Vertigan, and D. J. A. Welsh, *On the computational complexity of the Jones and Tutte polynomials*, Math. Proc. Cambridge Philos. Soc. **108** (1990), no. 1, 35–53. MR MR1049758 (91h:05038)
- [Lad75] Richard E. Ladner, *On the structure of polynomial time reducibility*, J. ACM **22** (1975), no. 1, 155–171.
- [Lin86] Nathan Linial, *Hard enumeration problems in geometry and combinatorics*, SIAM J. Algebraic Discrete Methods **7** (1986), no. 2, 331–335. MR MR830652 (87e:68029)
- [Lov67] László Lovász, *Operations with structures*, Acta Math. Acad. Sci. Hungar. **18** (1967), 321–328. MR MR0214529 (35 #5379)
- [Lov06] ———, *The rank of connection matrices and the dimension of graph algebras*, Eur. J. Comb. **27** (2006), no. 6, 962–970.
- [LS08] László Lovász and Alexander Schrijver, *Graph parameters and semigroup functions*, European J. Combin. **29** (2008), no. 4, 987–1002. MR MR2408373 (2008m:05179)
- [Mat79] Rudolf Mathon, *A note on the graph isomorphism counting problem*, Inf. Process. Lett. **8** (1979), no. 3, 131–132.

- [PB83] J. Scott Provan and Michael O. Ball, *The complexity of counting cuts and of computing the probability that a graph is connected*, SIAM J. Comput. **12** (1983), no. 4, 777–788.
- [Ric01] Daniel Richardson, *Multiplicative independence of algebraic numbers and expressions*, J. Pure Appl. Algebra **164** (2001), no. 1-2, 231–245, Effective methods in algebraic geometry (Bath, 2000). MR MR1854340 (2002j:11079)
- [Sch78] Thomas J. Schaefer, *The complexity of satisfiability problems*, STOC, ACM, 1978, pp. 216–226.
- [Sch09] Alexander Schrijver, *Graph invariants in the spin model*, Journal of Combinatorial Theory, Series B **99** (2009), no. 2, 502 – 511.
- [Sim77] Janos Simon, *On the difference between one and many (preliminary version)*, ICALP (Arto Salomaa and Magnus Steinby, eds.), Lecture Notes in Computer Science, vol. 52, Springer, 1977, pp. 480–491.
- [Thu09] Marc Thurley, *The complexity of partition functions*, Ph.D. thesis, Humboldt Universität zu Berlin, 2009.